NEC-1627PCT
PCT/JP2004/019593
28.12.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

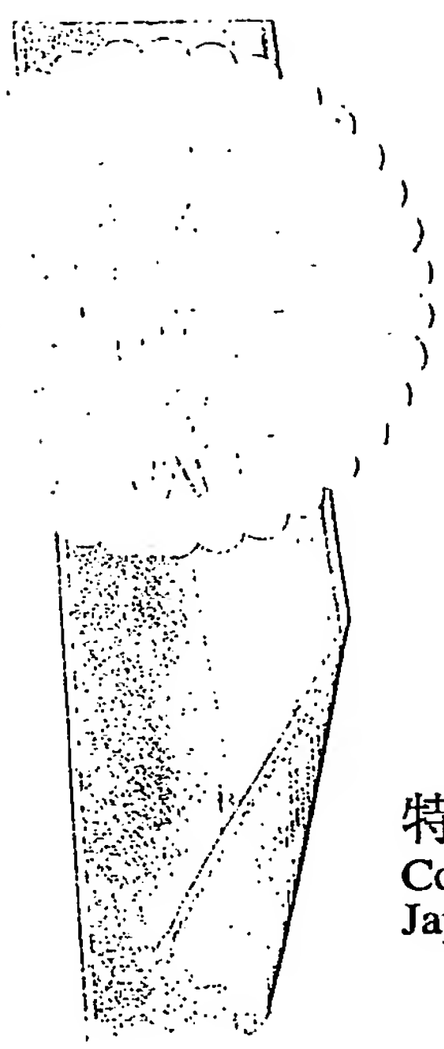
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００４年 １月１４日

出 願 番 号
Application Number: 特願２００４－００６５４２

[ST. 10/C]: [ＪＰ２００４－００６５４２]

出 願 人
Applicant(s): 日本電気株式会社



２００４年１０月 ８日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋

出証番号 出証特２００４－３０９１０５５

【書類名】　特許願
【整理番号】　33510051
【提出日】　平成16年 1月14日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/32
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　石川　雄一
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　藤田　範人
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　飯島　明夫
【発明者】
　【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
　【氏名】　岩田　淳
【特許出願人】
　【識別番号】　000004237
　【氏名又は名称】　日本電気株式会社
【代理人】
　【識別番号】　100088959
　【弁理士】
　【氏名又は名称】　境　廣巳
【手数料の表示】
　【予納台帳番号】　009715
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9002136

【書類名】特許請求の範囲
【請求項１】
カーネル部に設けられたデータ送受信部の暗号化機能を用い、アプリケーションがネットワークに接続された他のノード装置と暗号化通信を行う方法において、
a)通信方式解決部が、前記アプリケーションが前記他のノードのIPアドレスを解決するために送信する名前解決クエリまたはその応答である名前解決応答に含まれるドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定するステップ、
b)暗号化通信路設定部が、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを暗号化通信路設定テーブルに登録するステップ、
c)名前解決クエリ・応答送受信部が、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを前記アプリケーションに送信するステップ、
d)前記アプリケーションが、宛先アドレスに前記他のノード装置のIPアドレスが設定されたデータパケットを送信するステップ、
e)前記データ送受信部が、前記アプリケーションより送信された前記データパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信するステップ、
を含むことを特徴とする暗号化通信方法。
【請求項２】
前記ステップa、b、cの処理が前記アプリケーションが動作するノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする請求項1記載の暗号化通信方法。
【請求項３】
前記ステップaの処理が名前解決サーバで実行され、前記ステップb、cの処理が前記アプリケーションが動作するノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする請求項1記載の暗号化通信方法。
【請求項４】
通信暗号化ノードのカーネル部に設けられたデータ送受信部の暗号化機能を用い、前記通信暗号化ノードとは別のノード上のアプリケーションがネットワークに接続された他のノード装置と暗号化通信を行う方法において、
a)通信方式解決部が、前記アプリケーションが前記他のノードのIPアドレスを解決するために送信する名前解決クエリまたはその応答である名前解決応答に含まれるドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定するステップ、
b)暗号化通信路設定部が、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を暗号化通信路設定テーブルに登録するステップ、
c)名前解決クエリ・応答送受信部が、前記名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信するステップ、
d)前記アプリケーションが、宛先アドレスに前記インターセプト用アドレスが設定されたデータパケットを送信するステップ、
e)前記データ送受信部が、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する前記暗号化通信路設定テーブルから、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを暗号化して送信するステップ、
を含むことを特徴とする暗号化通信方法。
【請求項５】
前記ステップa、b、cの処理が前記暗号化通信ノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする請求項4記載の暗号化通信方法。

【請求項６】
前記ステップaの処理が名前解決サーバで実行され、前記ステップb、cの処理が前記暗号化通信ノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする請求項4記載の暗号化通信方法。
【請求項７】
前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする請求項1または4記載の暗号化通信方法。
【請求項８】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、
カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、
前記名前解決プロキシ部は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とするノード装置。
【請求項９】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、
カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
前記名前解決プロキシ部は、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とするノード装置。
【請求項１０】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、
前記ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブル

と、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、
　前記名前解決サーバは、名前解決に関連する機能に加えて、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部を備え、
　前記名前解決プロキシ部は、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする暗号化通信システム。
【請求項１１】
　ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、
　カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、
　前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とするノード装置。
【請求項１２】
　ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、
　前記ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
　前記名前解決サーバは、名前解決に関連する機能に加えて、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報を前記名前解決応答に付加して送信する名前解決応答・クエリ送受信部とを備え、
　前記名前解決プロキシ部は、前記暗号化通信路設定情報が付加された前記名前解決応答を前記名前解決サーバから受信したときに、前記暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする暗号化通信システム。

【請求項１３】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、
カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスと前記暗号化通信路設定情報との対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とするノード装置。
【請求項１４】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、
カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを暗号化して送信する通信暗号化部とを備え、
前記名前解決プロキシ部は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする通信暗号化ノード装置。
【請求項１５】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、
カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答

である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
　前記名前解決プロキシ部は、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする通信暗号化ノード装置。
【請求項１６】
　ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、
　前記通信暗号化ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定した前記データパケットを暗号化して送信する通信暗号化部とを備え、
　前記名前解決サーバは、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部を備え、
　前記名前解決プロキシ部は、前記他のノード装置が暗号化通信対象ノードである場合に、前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする暗号化通信システム。
【請求項１７】
　ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、
　カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装

置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定した前記データパケットを暗号化して送信する通信暗号化部とを備え、
　前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする通信暗号化ノード装置。
【請求項１８】
　ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、
　前記通信暗号化ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
　前記名前解決サーバは、名前解決に関連する機能に加えて、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報を前記名前解決応答に付加して送信する名前解決応答・クエリ送受信部とを備え、
　前記名前解決プロキシ部は、前記暗号化通信路設定情報が付加された前記名前解決応答を前記名前解決サーバから受信したときに、前記暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリ

ケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする暗号化通信システム。

【請求項１９】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと暗号化通信路設定情報と他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする通信暗号化ノード装置。

【請求項２０】

前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする請求項8または14記載のノード装置。

【請求項２１】

前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする請求項10または16記載の暗号化通信システム。

【請求項２２】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置を構成するコンピュータを、

カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、

前記通信暗号化手段は、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信するものであり、

前記名前解決プロキシ手段は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノー

ドかどうかを判定する通信方式解決手段と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。
【請求項２３】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置を構成するコンピュータを、
カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、
前記通信暗号化手段は、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信するものであり、
前記名前解決プロキシ手段は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決手段と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。
【請求項２４】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置を構成するコンピュータを、
カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、
前記通信暗号化手段は、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信するものであり、
前記名前解決プロキシ手段は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信手段と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。
【請求項２５】
ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置を構成するコンピュータを、
カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、
前記通信暗号化手段は、前記アプリケーションより送信されたデータパケットを受信し

、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信するものであり、

前記名前解決プロキシ手段は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信手段と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスと前記暗号化通信路設定情報との対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。

【請求項２６】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置を構成するコンピュータを、

カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、

前記通信暗号化手段は、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを暗号化して送信するものであり、

前記名前解決プロキシ手段は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決手段と、前記他のノード装置が暗号化通信対象ノードである場合に、前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信手段とを備えることを特徴とするプログラム。

【請求項２７】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置を構成するコンピュータを、

カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、

前記通信暗号化手段は、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルから読み出し、前記データパケットの宛

先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信するものであり、
前記名前解決プロキシ手段は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決手段と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信手段とを備えることを特徴とするプログラム。

【請求項２８】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置を構成するコンピュータを、
カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、
前記通信暗号化手段は、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定した前記データパケットを暗号化して送信するものであり、
前記名前解決プロキシ手段は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信手段と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。

【請求項２９】

ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置を構成するコンピュータを、
カーネル部のデータ送受信部に設けられた通信暗号化手段、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ手段、として機能させるプログラムであり、
前記通信暗号化手段は、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情

報との対応を保持する暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信するものであり、

前記名前解決プロキシ手段は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信手段と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと暗号化通信路設定情報と他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定手段とを備えることを特徴とするプログラム。

【請求項３０】

前記通信方式解決手段は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする請求項22または26記載のプログラム。

【書類名】明細書
【発明の名称】暗号化通信方法、暗号化通信システム、ノード装置及びプログラム
【技術分野】
【０００１】
本発明は、不特定多数のノードが接続されているオープンなネットワーク上において特定のグループに属する複数のノード間で相互にセキュアな通信を行う暗号化通信方法に関する。
【背景技術】
【０００２】
従来より、RFC2401やRFC3546等に記載されているように、不特定多数のノードが接続されているオープンなネットワーク（インターネット、公衆ホットスポットなど）上において、ノード、サーバ、ゲートウェイ装置などのノード間で通信を暗号化し、外部の第３者が通信内容を覗き見ることができないセキュアな通信路を提供するために、種々の暗号化通信方法が利用されている。
【０００３】
この種の暗号化通信方法を実現する通信暗号化プロトコルの例としては、暗号化するレイヤによって、以下のように大別される。
○レイヤ４（トランスポートレイヤ）以上
SSL(Secure Socket Layer)、TLS(Transport Layer Security)、SSH(Secure Shell)
○レイヤ３（ネットワークレイヤ）以下
IPsec、L2TP(Layer 2 Tunneling Protocol) over IPsec、Ethernet(登録商標) over IPsec
【０００４】
これらの通信暗号化プロトコルを利用し、他のノードと暗号化された通信を行う場合、従来の暗号化通信方法は、通信暗号化の形態により以下の3つに分類できる。
（１）Webブラウザや電子メールアプリケーションなどの個々のアプリケーションにおいて通信暗号化を行う形態
（２）通信暗号化モジュールを利用して通信暗号化を行う形態
（３）OS(Operating System)のカーネル部が提供する機能を利用して通信暗号化を行う形態
【０００５】
形態（１）の暗号化通信方法の場合、前述したレイヤ4以上の通信暗号化プロトコルが利用される。例えば、“example.com”のドメインネームをもつ通信相手に対して、HTTP(Hyper Text Transfer Protocol)通信を暗号化したい場合、Webブラウザにおいて、“https://example.com/index.html”などのURL(Universal Resource Locator)を入力し、通信相手とのHTTP通信をSSLで暗号化する。このような通信暗号化形態は、当然ながら、アプリケーションが通信暗号化プロトコルをサポートしない限り利用することが出来ない。
【０００６】
形態（２）の通信暗号化モジュールを利用して通信暗号化を行う場合、主に前述したレイヤ4以上の通信暗号化プロトコルが利用される。通信暗号化モジュールは、独立したプロセスとして動作し、アプリケーションと通信相手とが送受信するデータパケットをインターセプトし、暗号化/復号化を行った後に通信相手/アプリケーションに送信する。通信暗号化モジュールの例としては、任意のTCP(Transport Control Protocol)コネクションをSSL暗号化するstunnelや、任意のTCPコネクションをSSHで暗号化トンネリングを行うSSHポートフォワーディングなどがある。
【０００７】
この形態（２）の通信暗号化方法では、形態（３）の通信暗号化方法と同様に、アプリケーションが通信暗号化プロトコルをサポートしているかどうかに依存することなく通信を暗号化することができるため、任意のアプリケーションの通信を暗号化することができる。さらに、この通信暗号化の形態においては、形態（３）の通信暗号化方法と異なりアプ

リケーションを意識した通信の暗号化が可能であり、特定のアプリケーションに関する通信のみ暗号化を行うといったことが可能である。

【０００８】

この形態（２）の通信暗号化方法による通信暗号化処理の概要を図10に示す。通信暗号化モジュールA13xは、通信の暗号化処理を行う通信暗号化部A131xと暗号化通信の対象ノード(以下、暗号化通信対象ノードと称す)C1のアドレスと暗号化通信路設定情報の組が唯一登録された暗号化通信路設定テーブルA132xとを含み、それ自体が独立したプロセスとして動作する。通信暗号化モジュールA13xにおいてアプリケーションA11xの送信したデータパケットに対して通信暗号化処理を行うためには、アプリケーションA11xがデータパケットを通信暗号化モジュールA13xに一旦渡し、必要な暗号化処理を行った後に、通信暗号化モジュールA13xがデータパケットを本来の通信相手へ送信する、という手順がとられる。そのため、アプリケーションA11xにおいては、通信相手として直接本来の通信相手のＩＰアドレスを指定するのではなく、ループバックアドレスである127.0.0.1（および必要に応じてプロセス（通信暗号化モジュール）の受信ポート番号）を宛先アドレスとして指定してデータパケットを送信し、通信暗号化モジュールA13xがデータパケットを受信できるようにする。通信暗号化モジュールA13xは、アプリケーションA11xからデータパケットを受信すると、通信暗号化部A131xの暗号・復号化処理部A1311xにより暗号化通信路設定テーブルA132xを参照し、予め設定されている通信相手(図10では、IPアドレス1.2.3.4のノード)に対して、暗号化通信路設定情報に従ってデータパケットを暗号化し(図10では、プロトコル：SSL、暗号化アルゴリズム:DES、電子証明書ID：11を利用する)、アドレス変換部A1312xにより宛て先をIPアドレス1.2.3.4に書き換えて送信する。

【０００９】

なお、本形態（２）の暗号化通信方法では、図10に示したようにクライアントノードA1xが内部に通信暗号化モジュールA13xを含む構成以外に、通信暗号化モジュールが通信暗号化プロキシノードとして外部のノードにおいて提供されている構成もある。この場合、アプリケーションはこの外部ノードのIPアドレスを宛先アドレスに指定してデータパケットを送信する。通信暗号化モジュールは受信したデータパケットに対して必要な暗号化処理を行った後、予め設定された通信相手(暗号化通信対象ノードのIPアドレスが指定される）へとデータパケットを送信する。

【００１０】

形態（３）のOSのカーネル部が提供する機能を利用して通信暗号化を行う暗号化通信方法の場合、主に前述したレイヤ3以下の通信暗号化プロトコルが利用される。例えば、1.2.3.4というIPアドレスをもつ通信相手との間で全てのIPパケットを暗号化したい場合、OSの設定において通信相手（IPアドレス＝1.2.3.4）との間にトランスポートモードまたはトンネリングモードでのIPsec設定を行う。

【００１１】

この形態（３）の暗号化通信方法では、形態（２）の暗号化通信方法と同様にアプリケーションが通信暗号化プロトコルをサポートしているかどうかに依存することなく通信を暗号化することができるため、任意のアプリケーションの通信を暗号化することができる。ただし本通信暗号化の形態（３）においては一般的に、形態（２）の暗号化通信方法と異なりアプリケーションを意識することなく、予め設定されたIPアドレスを持つ通信相手との通信が全て暗号化されるため、特定のアプリケーションに関する通信のみ暗号化を行うといったことはできない。

【００１２】

この形態（３）の暗号化通信方法における通信暗号化処理の概要を図11に示す。通信の暗号化処理を行う通信暗号化部A141yと暗号化通信対象ノードのアドレスおよび暗号化通信路の設定情報が登録された暗号化通信路設定テーブルA142yは、OSのカーネル部内のデータ送受信部A14yに含まれる。アプリケーションA11xが送信する全てのデータパケットは送信処理のためデータ送受信部A14yに渡され、データ送受信部A14y内の通信暗号化部A141yが、データパケットの宛先アドレスを元に暗号化通信路設定テーブルA142yを参照し、宛

先アドレスが暗号化通信対象ノードとして登録されている場合(図11においては宛先アドレスが1.2.3.4、5.6.7.8の場合)は、登録されている暗号化通信路設定情報(図11においては、例えばプロトコル:IPSec、暗号化アルゴリズム:DES、電子証明書ID:11)に従って、暗号化処理を行い通信相手に送信する。

【発明の開示】

【発明が解決しようとする課題】

【００１３】

前述したOSが提供する通信暗号化機能を利用した暗号通信方法は、アプリケーションが通信暗号化プロトコルをサポートしているかどうかに依存することなく通信暗号化を実現することができ、かつ、前述した通信暗号化モジュールを利用する暗号化通信方法とは異なり、暗号化通信を行う相手(以下、暗号化通信対象ノードと称す)のIPアドレスを予め複数設定することで、複数の通信相手と暗号化通信を行うことが可能である。しかしながら、暗号化通信対象ノードの設定のためのコストが大きいという問題点がある。以下、この問題点について詳述する。

【００１４】

インターネットのような不特定多数のノードが接続されているオープンなネットワークにおいて、複数の通信相手と暗号化通信を行う場合、どの通信相手が暗号化通信対象ノードなのかを指定する必要がある。IPネットワークにおいて相手ノードを示す識別子としては、ドメインネームとIPアドレスがある（ドメインネームによって相手を指定する場合は、DNS(Domain Name System)によってドメインネームに対応するIPアドレスの解決を行う必要がある）。しかしながら、通信相手の指定にこれらの識別子を利用することは以下の理由により不可能である。

【００１５】

○IPアドレス

暗号化通信対象ノードの数が多い場合、相手のIPアドレスの数だけ設定を行わなければならないため、その設定は非常にコストがかかる。IPアドレス範囲(IPアドレススコープとも言う。例えば192.168.1.0/24等)を利用することで、複数の暗号化通信対象ノードの設定を集約することは可能だが、この場合、集約できるのは当然ながら共通のIPアドレス範囲に属する暗号化通信対象ノードの設定に限られる。このため、IPアドレスに依らずに、任意の暗号化通信対象ノードによってグループを構成し、グループ単位で設定を集約するといったことは出来ない。また、一般的にノードのIPアドレスはDHCPなどの機構によって動的に変化することがあるため、相手ノードのIPアドレスの変化に対応して設定を動的に変えるのは非現実的である。

【００１６】

○ドメイン名

ドメイン名による指定が可能であれば、暗号化通信対象ノードのIPアドレスがDHCPなどの機構によって動的に変化したとしても、設定を変更する必要はない。さらに、ドメイン名条件(ドメインサフィックスやドメインプレフィックスなど)による指定が可能であれば、ネットワーク上の位置に拠らずに、任意の暗号化通信対象ノードによってグループを構成し、グループ単位で設定を集約するといったことが可能となる。

【００１７】

ここで、OSのカーネル部に含まれる通信暗号化部(図11におけるA141y)はデータパケットに含まれる情報から通信相手のノード種別を判断するが、アプリケーションが送信するデータパケットには、一般的にドメイン名は含まれない。このため、暗号化通信を行うべき相手の指定にドメイン名を用いることは従来技術では不可能である。場合によっては、データパケットのレイヤ7のヘッダ部分(HTTPのRequestヘッダ等)やデータグラム内部に、通信相手のドメイン名が含まれることがあるが、これらの情報に基づいて通信相手識別を行うためには、通信暗号化モジュールにおいて個々のアプリケーションに特化した機能拡張が必要となるため非現実的である。

【００１８】

本発明の目的は、OSが提供する通信暗号化機能を利用して複数の通信相手と暗号化通信を行う場合の暗号化通信対象ノードの設定コストを低減することにある。

【００１９】

本発明の別の目的は、暗号化通信対象ノードの設定において、設定項目や設定手順の数が暗号化通信対象ノードの数やIPアドレス、グループを構成するノードの変更頻度に依存しない(すなわち設定コストが一定の)設定方式を具備した、OSのカーネル部の通信暗号化機能を利用した暗号化通信方法を提供することである。

【課題を解決するための手段】

【００２０】

請求項1記載の暗号化方法は、カーネル部に設けられたデータ送受信部の暗号化機能を用い、アプリケーションがネットワークに接続された他のノード装置と暗号化通信を行う方法において、

a)通信方式解決部が、前記アプリケーションが前記他のノードのIPアドレスを解決するために送信する名前解決クエリまたはその応答である名前解決応答に含まれるドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定するステップ、

b)暗号化通信路設定部が、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを暗号化通信路設定テーブルに登録するステップ、

c)名前解決クエリ・応答送受信部が、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを前記アプリケーションに送信するステップ、

d)前記アプリケーションが、宛先アドレスに前記他のノード装置のIPアドレスが設定されたデータパケットを送信するステップ、

e)前記データ送受信部が、前記アプリケーションより送信された前記データパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信するステップ、

を含むことを特徴とする。

【００２１】

請求項2記載の暗号化通信方法は、請求項1記載の暗号化通信方法において、前記ステップa、b、cの処理が前記アプリケーションが動作するノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする。

【００２２】

請求項3記載の暗号化通信方法は、請求項1記載の暗号化通信方法において、前記ステップaの処理が名前解決サーバで実行され、前記ステップb、cの処理が前記アプリケーションが動作するノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする。

【００２３】

請求項4記載の暗号化通信方法は、通信暗号化ノードのカーネル部に設けられたデータ送受信部の暗号化機能を用い、前記通信暗号化ノードとは別のノード上のアプリケーションがネットワークに接続された他のノード装置と暗号化通信を行う方法において、

a)通信方式解決部が、前記アプリケーションが前記他のノードのIPアドレスを解決するために送信する名前解決クエリまたはその応答である名前解決応答に含まれるドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定するステップ、

b)暗号化通信路設定部が、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を暗号化通信路設定テーブルに登録するステップ、

c)名前解決クエリ・応答送受信部が、前記名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信するステップ、

d)前記アプリケーションが、宛先アドレスに前記インターセプト用アドレスが設定されたデータパケットを送信するステップ、

e)前記データ送受信部が、前記アプリケーションより送信された宛先アドレスにインタ

ーセプト用アドレスが設定されたデータパケットを受信し、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する前記暗号化通信路設定テーブルから、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを暗号化して送信するステップ、
を含むことを特徴とする。

【００２４】

請求項5記載の暗号化通信方法は、請求項4記載の暗号化通信方法において、前記ステップa、b、cの処理が前記暗号化通信ノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする。

【００２５】

請求項6記載の暗号化通信方法は、請求項4記載の暗号化通信方法において、前記ステップaの処理が名前解決サーバで実行され、前記ステップb、cの処理が前記暗号化通信ノード装置に設けられた名前解決プロキシ部で実行されることを特徴とする。

【００２６】

請求項7記載の暗号化通信方法は、請求項1または4記載の暗号化通信方法において、前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする。

【００２７】

請求項8記載のノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする。

【００２８】

請求項9記載のノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチし

たドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする。

【００２９】

請求項10記載の暗号化通信システムは、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、

前記ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、

前記名前解決サーバは、名前解決に関連する機能に加えて、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部を備え、

前記名前解決プロキシ部は、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする。

【００３０】

請求項11記載のノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスを複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、前記データパケットを暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスを前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする。

【００３１】

請求項12記載の暗号化通信システムは、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、

前記ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信

路設定情報に従って暗号化して送信する通信暗号化部とを備え、
　前記名前解決サーバは、名前解決に関連する機能に加えて、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報を前記名前解決応答に付加して送信する名前解決応答・クエリ送受信部とを備え、
　前記名前解決プロキシ部は、前記暗号化通信路設定情報が付加された前記名前解決応答を前記名前解決サーバから受信したときに、前記暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする。
【００３２】
　請求項13記載のノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するノード装置において、
　カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信されたデータパケットを受信し、前記データパケットの宛先アドレスに設定された通信相手IPアドレスが前記暗号化通信路設定テーブルに登録されていた場合に、対応する暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、
　前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを含む名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記他のノード装置のIPアドレスと前記暗号化通信路設定情報との対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部を備えることを特徴とする。
【００３３】
　請求項14記載の通信暗号化ノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、
　カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、
　前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを暗号化して送信する通信暗号化部とを備え、
　前記名前解決プロキシ部は、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セ

ッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする。

【００３４】

請求項15記載の通信暗号化ノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする。

【００３５】

請求項16記載の暗号化通信システムは、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、

前記通信暗号化ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定した前記データパケットを暗号化して送信する通信暗号化部とを備え、

前記名前解決サーバは、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名に基づいて、前記他のノード装置が暗号化通信対象ノードかどうかを判定する通信方式解決部を備え、

前記名前解決プロキシ部は、前記他のノード装置が暗号化通信対象ノードである場合に

、前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部と、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする。

【００３６】

請求項17記載の通信暗号化ノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスとの対応を複数保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレスを前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定した前記データパケットを暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする。

【００３７】

請求項18記載の暗号化通信システムは、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するための名前解決サーバとを備え、

前記通信暗号化ノード装置は、カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために前記名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、

前記名前解決サーバは、名前解決に関連する機能に加えて、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記

名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報を前記名前解決応答に付加して送信する名前解決応答・クエリ送受信部とを備え、

前記名前解決プロキシ部は、前記暗号化通信路設定情報が付加された前記名前解決応答を前記名前解決サーバから受信したときに、前記暗号化通信路設定情報と前記名前解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部とを備えることを特徴とする。

【００３８】

請求項19記載の通信暗号化ノード装置は、ネットワークに接続された他のノード装置と通信を行うアプリケーションが動作するクライアントノード装置に前記ネットワークを通じて接続された通信暗号化ノード装置において、

カーネル部に設けられたデータ送受信部と、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部とを備え、

前記データ送受信部は、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を前記暗号化通信路設定テーブルから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部とを備え、

前記名前解決プロキシ部は、前記アプリケーションが前記他のノード装置のIPアドレスを解決するために送信した前記名前解決クエリを前記名前解決サーバに送信し、前記他のノード装置が暗号化通信対象ノードかどうかの判定結果と暗号化通信路設定情報と前記他のノード装置のIPアドレスとを含む名前解決応答を前記名前解決サーバから受信し、前記他のノード装置が暗号化通信対象ノードであると判定された場合に、前記名前解決応答に含まれる前記他のノード装置のIPアドレスを、前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応中の前記インターセプト用アドレスに置き換えた名前解決応答を前記アプリケーションに送信する名前解決クエリ・応答送受信部と、前記他のノード装置が暗号化通信対象ノードである場合に、前記他のノード装置のIPアドレスと暗号化通信路設定情報と他の通信セッションで使用されていないインターセプト用アドレスとの対応を前記暗号化通信路設定テーブルに登録する暗号化通信路設定部とを備えることを特徴とする。

【００３９】

請求項20記載のノード装置は、請求項8、10または14記載のノード装置において、前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする。

【００４０】

請求項21記載の暗号化通信システムは、請求項16記載の暗号化通信システムにおいて、前記通信方式解決部は、暗号化通信の対象ノードのドメイン名の全体または一部が登録された設定テーブルを参照して、前記他のノード装置が暗号化通信対象ノードかどうかを判定することを特徴とする。

【発明の効果】

【００４１】

本発明によれば、OSが提供する通信暗号化機能を利用して複数の通信相手と暗号化通信を行う場合の暗号化通信対象ノードの設定コストを低減することができる。その理由は、アプリケーションが通信相手のIPアドレスを解決するために送信する名前解決クエリまたはその応答である名前解決応答に含まれるドメイン名に基づいて、通信相手のノード種別を判断するためである。

【発明を実施するための最良の形態】

【００４２】

次に、本発明の第一の実施の形態について図面を参照して詳細に説明する。

【００４３】

図1を参照すると、本発明の第一の実施の形態は、クライアントノードA1aとDNS(Domain Name System)サーバB1aと暗号化通信対象ノードC1と通常通信対象ノードD1とによって実現される。クライアントノードA1aとDNSサーバB1aと暗号化通信対象ノードC1と通常通信対象ノードD1はネットワークE1を介して接続されている。ここで、暗号化通信対象ノードC1は、クライアントノードA1aとの間で暗号化通信を行うノード、通常通信対象ノードD1は、クライアントノードA1aとの間で暗号化されていない通常の通信を行うノードである。

【００４４】

クライアントノードA1aは、アプリケーションA11xと、DNS Proxy部A12aと、データ送受信部A14aとを含む。データ送受信部A14aはデータパケットの送受信を行う部分で、カーネル部に設けられている。

【００４５】

アプリケーションA11xは、Webブラウザや電子メールソフトや、ビデオ会議ソフトなどコンピュータを使って、それぞれの目的を実現するためのソフトウェアであり、通信相手の名前をIPアドレスに解決するよう要求する機能を有する。

【００４６】

ここで、本明細書の記載において、「名前」とは、一つまたは複数の、IPアドレスまたはIPアドレス範囲が、直接的または間接的に対応付けられている全ての識別子を意味する(すなわち、「名前」を与えられると、直接的または間接的に、一つまたは複数の、IPアドレスまたはIPアドレス範囲を特定することができることを意味する。ここで、IPアドレスまたはIPアドレス範囲から「名前」を特定できる必要は必ずしも無い)語として用いる。例えば以下のような識別子が「名前」に該当する。

・A←→1.2.3.4 という対応関係を持つ識別子A(1.2.3.4はIPアドレスの例)
・B←→1.2.3.0/24 という対応関係を持つ識別子B(1.2.3.0/24はIPアドレス範囲の例)
・C←→1.2.3.4　C←→5.6.7.8 という対応関係を持つ識別子C
・D←→A という対応関係を持つ識別子D

現状インターネットで利用されている名前の代表例としては、ドメイン名(例えばsato.biglobe.ne.jpやsuzuki.nec.com等が挙げられる。ドメイン名はFQDN(Fully Qualified Domain Name)とも呼ばれる)が挙げられる。

【００４７】

また、名前から名前に対応付けられた一つまたは複数の、IPアドレスまたはIPアドレス範囲を特定することは、一般的に名前解決と呼ばれる。名前解決を行う仕組みとして代表的なものにDNSが挙げられる。DNSを利用することで、ドメイン名をIPアドレスに解決することが出来る。この他にもNIS(Network Information Service)や、WINS(Windows(登録商標) Internet Name Service)などが、名前解決を行う仕組みの例として挙げられる。本明細書においては、「名前解決」を上記の例に限定せず、「名前から名前に対応付けられた一つまたは複数の、IPアドレスまたはIPアドレス範囲を特定すること」全てを意味する語として用いる(例えば、文字列を入力するとその文字列に対応付けられたIPアドレスを表示するようなCGI(Common Gateway Interface)を有するWebサーバも名前解決を行う仕組みに該当する)。

【００４８】

以下の説明では、説明を簡単にするため、名前としてドメイン名を、名前解決を行う仕組

みとしてDNSをそれぞれ例にとり説明するが、以下の説明は全ての名前および名前解決を行う仕組みに適用することが可能である。適用する際には、以下の説明においてドメイン名を名前に、DNSを名前解決にそれぞれ読み替える(例えばDNSサーバ→名前解決サーバ、DNSクエリメッセージ→名前解決クエリメッセージ、DNSレスポンスメッセージ→名前解決レスポンスメッセージ等)ものとする。

【００４９】

さて、本実施の形態においてアプリケーションA11xは、DNS Proxy部A12aに割り当てられたループバックアドレス(例えば127.0.0.1)宛にDNSクエリメッセージを送信することで通信相手のドメイン名→IPアドレスの解決を要求する。従って、アプリケーションA11xが送信したDNSクエリメッセージは、DNS Proxy部A12aが受信することになる。なお、ループバックアドレスとは、自ノード内で閉じた通信を行うために利用されるIPアドレスのことであり、一般的には127.0.0.0/8の範囲にあるIPアドレスが該当する。

【００５０】

アプリケーションA11xは、DNS Proxy部A12aより受信したDNSレスポンスメッセージの名前解決結果に含まれるIPアドレスを送信データパケットの宛先アドレスに指定して、データを送信する。

【００５１】

なお、一般的にアプリケーションからの名前解決要求を受けてDNSクエリメッセージを作成・送信する機能、及びDNSサーバより受信したDNSレスポンスメッセージから名前解決結果を取得してアプリケーションに渡す機能は、ノードの基本ソフトウェア(OS(Operating System)とも呼ぶ)のシステム関数として提供されることが多いが、本明細書では前記も含め、説明を簡単にするために「アプリケーションがDNSメッセージを送・受信する」と表現することにする。

【００５２】

DNS Proxy部A12aは、DNSクエリ・応答送受信部A121aと、通信方式解決部A122aと、暗号化通信路設定部A123aと、DNSサーバアドレス設定テーブルA124aと、CUG(Closed User Group)設定テーブルA125aとを含む。

【００５３】

DNS Proxy部A12aは、アプリケーションA11xによる名前解決要求を受けてアプリケーションA11xの通信相手のIPアドレスをDNSサーバB1aにより解決すると共に、通信相手のノード種別(通信相手のノード種別とは、通信相手が暗号化通信対象ノードであるか通常通信の対象ノード(以下、通常通信対象ノードと称す)であるかの種別を意味する)を判断し、通信相手が暗号化通信対象ノードである場合には、暗号化通信対象ノードのIPアドレスをデータ送受信部A14aに設けられる暗号化通信路設定テーブルA142aに登録する機能を有する。通信相手が通常通信対象ノードの場合は、このような登録は行われない。

【００５４】

以下、DNS Proxy部A12aの構成について説明する。まずDNSクエリ・応答送受信部A121aについて説明する。

【００５５】

DNSクエリ・応答送受信部A121aは、アプリケーションA11xからDNSクエリメッセージを受信すると、DNSサーバアドレス設定テーブルA124aに登録されている外部DNSサーバB1aに対してDNSクエリメッセージを送信する。DNSクエリメッセージの応答として、外部DNSサーバB1aからDNSレスポンスメッセージを受信すると、DNSレスポンスメッセージに含まれる名前解決結果を通信方式解決部A122aに渡す。通信方式解決部A122aに渡す名前解決結果には、名前解決の対象となったドメイン名(つまりアプリケーションA11xの通信相手のドメイン名)や解決されたIPアドレス(つまり通信相手のIPアドレス)が含まれる。通信方式解決部A122aに名前解決結果を渡したDNSクエリ・応答送受信部A121aは、アプリケーションA11xに対してDNSレスポンスメッセージを送信する。

【００５６】

次に通信方式解決部A122aについて説明する。通信方式解決部A122aは、DNSクエリ・応答

送受信部A121aから渡された名前解決結果を元にCUG設定テーブルA125aを参照し、アプリケーションA11xの通信相手のノード種別を判断する。さらに、アプリケーションA11xの通信相手が暗号化通信対象ノードである場合には、CUG設定テーブルA125aを参照して当該通信相手の通信に用いる暗号化通信路の設定情報を把握する。

【００５７】

ここで、通信方式解決部A122aは、ノード種別判断に用いる通信相手の識別子として、ドメイン名を利用する。ドメイン名を用いてアプリケーションA11xの通信相手のノード種別を判断する場合、通信方式解決部A122aは、通信相手のドメイン名の全てまたは一部がCUG設定テーブルA125aにおいて暗号化通信対象ノードのドメイン名として登録されているか否かをチェックする。例えば、通信相手のドメイン名がsato.biglobe.ne.jpである場合は、CUG設定テーブルA125aにおいてドメイン名 sato.biglobe.ne.jpまたは、sato.biglobe.ne.jpが該当するドメイン名条件(例えばsato.*(前方ラベルがsatoであるドメイン名を示す)のようなドメインプレフィックスや、*.biglobe.ne.jp(後方ラベルがbiglobe.ne.jpであるドメイン名を示す)のようなドメインサフィックス、*.biglobe.*(biglobeというラベルを含む任意のドメイン名を示す）のような任意のドメイン名条件などが挙げられる）が暗号化通信対象ノードのドメイン名として登録されているか否かをチェックする。

【００５８】

通信方式解決部A122aは、上記のような方法で、アプリケーションA11xの通信相手のノード種別を判断した後、暗号化通信対象ノードであると判断した場合、DNSクエリ・応答送受信部A121aから渡された名前解決結果及び通信相手との通信に用いる暗号化通信路設定情報を暗号化通信路設定部A123aに渡す。

【００５９】

次に暗号化通信路設定部A123aについて説明する。暗号化通信路設定部A123aは、データ送受信部A14aに含まれる暗号化通信路設定テーブルA142aに、暗号化通信対象ノードのIPアドレスと当該暗号化通信対象ノードとの通信に利用する暗号化通信路設定情報とを登録する機能を有する。具体的に、暗号化通信路設定部A123aは、通信方式解決部A122aから渡されたアプリケーションA11xの通信相手の名前解決結果に含まれる通信相手のIPアドレス及び、その通信相手との通信に用いる暗号化通信路設定情報を、暗号化通信路設定テーブルA142aに登録する。

【００６０】

次にDNSサーバアドレス設定テーブルA124aについて説明する。DNSサーバアドレス設定テーブルA124aには、外部DNSサーバB1aのアドレスが登録される。DNSサーバアドレス設定テーブルA124aは、DNSクエリ・応答送受信部Ａ121aがDNSクエリメッセージを送信する際に参照される。

【００６１】

次に、CUG設定テーブルA125aについて説明する。CUG設定テーブルA125aには、クライアントノードA1が参加するCUG(Closed User Group)に関する情報が登録されている。ここでCUGとは二つ以上の特定のノードから構成されるグループのことであり、グループ内の通信は暗号化され、グループ外の第三者からはのぞき見られないようになっている。すなわち、クライアントノードA1aが参加するCUGの他のノードは、クライアントノードA1aにとって暗号化通信対象ノードとなる。CUG設定テーブルA125aは、通信方式解決部A122aがアプリケーションA11xの通信相手のノード種別を判断する際に参照される。具体的には、CUG設定テーブルA125aには、クライアントノードA1aが参加しているCUGのノード(つまり暗号化通信対象ノード)の識別情報が登録される。CUG設定テーブルA125aに登録されるノードの識別情報は、ドメイン名条件である。例えば、*.myfriends.comが登録されている場合は、*.myfriends.comに該当するドメイン名(例えばsato.myfriends.com)を持つ通信相手が暗号化通信対象ノードとなる。

【００６２】

その他、CUG設定テーブルA125aには必須の登録情報ではないが、CUGのノードと通信をする際に利用する暗号化通信路の設定情報を登録しておくこともできる。暗号化通信路の設

定情報としては、具体的には例えば、通信プロトコル(例えばIPSecやSSL(Secure Socket Layer)、TLS(Transport Layer Security)等)と電子証明書ID(電子証明書とは自身の存在を証明するための電子的な証明書であり、例えば、ITU-T(International Telecommunication Union-Telecommunication Standardization Sector)勧告のX.509等が挙げられる。本説明において電子証明書のIDとは、アプリケーションA11xがセッションで利用すべき電子証明書を選択するために利用する識別子を意味する)、暗号化アルゴリズム(例えばDES(Data Encryption Standard)や3DES(triple-DES)、AES(Advanced Encryption Standard)等)などが使用される。

【００６３】

CUG設定テーブルA125aの例を図2に示す。図2に示すCUG設定テーブル201には、暗号化通信対象ノードの識別情報としてドメイン名条件が、暗号化通信路の設定情報として通信プロトコルと電子証明書ID、暗号化アルゴリズムがそれぞれ登録されている。例えば、図2に示すCUG設定テーブル201の4番目のエントリには、*.myfriends.comのドメイン名条件に該当するドメイン名を持つ通信相手ノード(例えば、yamada.myfriends.comやsato.myfriends.com)が暗号化通信対象ノードであり、それらのノードとは、通信プロトコル:SSL、電子証明書ID:11、暗号化アルゴリズム:DESを用いて暗号化通信を行うという設定がなされている。

【００６４】

DNS Proxy部A12aがCUG設定テーブルA125aとして図2で示したテーブル201を保持している場合、通信方式解決部A122aは通信相手のノード種別を通信相手のドメイン名を利用して判断する。例えば、通信相手のドメイン名が、taro.nec.co.jpである場合、当該ドメイン名は、テーブル201の2番目のエントリに登録されており、このため、通信方式解決部A122aは、通信相手が暗号化通信対象ノードであると判断する。通信相手のドメイン名が、yamada.myfriends.comである場合、当該ドメイン名自体はテーブル201に登録されていないが、ドメインサフィックス：myfriends.comがテーブル201の4番目のエントリに登録されているため、この場合も通信方式解決部A122aは通信相手が暗号化通信対象ノードであると判断する。通信相手のドメイン名がテーブル201に登録されているドメイン名のいずれにも合致しない場合、通信方式解決部A122aは通信相手が通常通信対象ノードであると判断する。

【００６５】

以上がDNS Proxy部A12aの構成である。

【００６６】

次にデータ送受信部A14aについて説明する。データ送受信部A14aは、通信暗号化部A141aと暗号化通信路設定テーブルA142aとを含む。アプリケーションA11xが外部のノードに対して送信する全てのデータパケットは、データ送受信部A14aによりインターセプトされ、送信処理が行われる。

【００６７】

通信暗号化部A141aは、データパケットの暗号・復号化処理を行う暗号・復号化処理部A1411aを有する。暗号・復号化処理部A1411aは、アプリケーションA11xから受信したデータパケットの宛先IPアドレスを元に暗号化通信路設定テーブルA142aを参照し、このテーブルに登録されている暗号化通信路設定情報に従って、受信したデータパケットに暗号化処理を施す機能を有する。また、外部の通信相手ノードから受信したデータパケットの送信元アドレスを元に暗号化通信路設定テーブルA142aを参照し、このテーブルに登録されている暗号化通信路設定情報に従って、受信したデータパケットに復号化処理を施す機能を有する。

【００６８】

次に暗号化通信路設定テーブルA142aについて説明する。暗号化通信路設定テーブルA142aには、暗号化通信対象ノードのIPアドレスと当該暗号化通信対象ノードとの通信に利用する暗号化通信路設定情報とが登録されている。登録は、暗号化通信路設定部A123aにより動的に行われる。暗号化通信路設定テーブルA142aの例を図3のテーブル301に示す。本例

では、通信相手のIPアドレスと暗号化通信路設定情報として通信プロトコル、電子証明書ID、暗号化アルゴリズムが登録されている。

【００６９】

データ送受信部A14aが暗号化通信路設定テーブルA142aとして図3に例示したテーブル301を保持していると仮定し、データ送受信部A14aが宛先アドレス133.11.64.24のデータパケットをインターセプトしたケースについて説明する。データ送受信部A14aがデータパケットをインターセプトすると、通信暗号化部A141aは暗号化通信路設定テーブルA142aを参照する。この場合、暗号化通信路設定テーブルA142aの2番目のエントリがインターセプトしたデータパケットに該当する。通信暗号化部A141aは、2番目のエントリに登録されている設定情報（通信プロトコル:IPSec、電子証明書ID:10、暗号化アルゴリズム:3DES）に従ってデータパケットを暗号化した後、送信する。

【００７０】

以上がデータ送受信部A14aの構成である。

【００７１】

次にDNSサーバB1aについて説明する。DNSサーバB1aは、DNSクエリメッセージにより要求された名前解決を行い、解決結果をDNSレスポンスメッセージによって要求元に通知する。DNSサーバB1aは、DNS応答・クエリ送受信部B11aと名前解決部B12aとアドレス解決用データベースB13aとを含み、これらはそれぞれ以下の機能を有する。

【００７２】

DNS応答・クエリ送受信部B11aは、クライアントノードA1aからDNSクエリメッセージを受信し、同メッセージに含まれる名前解決要求を名前解決部B12aに渡す。また、名前解決部B12aから渡された名前解決結果をDNSレスポンスメッセージによってクライアントノードA1に通知する。

【００７３】

名前解決部B12aは、アドレス解決用データベースB13aを参照してDNS応答・クエリ送受信部B11aから渡された名前解決要求に対する解決処理を行い、名前解決結果をDNS応答・クエリ送受信部B11aに渡す。

【００７４】

アドレス解決用データベースB13aは、ドメイン名とそれに対応するIPアドレスが登録されている。

【００７５】

次に、本実施の形態において、アプリケーションA11xが暗号化通信対象ノードC1または通常通信対象ノードD1と通信を行う際のクライアントノードA1aの動作について詳細に説明する。

【００７６】

クライアントノードA1aの動作は、アプリケーションA11xが通信相手のドメイン名に対する名前解決要求を行った際の動作と、通信相手に対してデータパケットを送信した際の動作に、大きく分けられる。

【００７７】

まず、アプリケーションA11xが名前解決要求を行う際のクライアントノードA1aの動作について説明する。

【００７８】

アプリケーションA11xは、ループバックアドレス宛(例えば127.0.0.1)に、DNSクエリメッセージを送信し、通信相手の名前解決を要求する。アプリケーションA11xが送信したDNSクエリメッセージは、DNS Proxy部A12a(具体的にはDNS Proxy部A12a内部のDNSクエリ・応答送受信部A121a)が受信する。その後の処理はDNS Proxy部A12aで行われる。

【００７９】

図4を参照して、DNS Proxy部A12aがアプリケーションA11xからDNSクエリメッセージを受信した際の動作について説明する。

【００８０】

アプリケーションA11xからDNSクエリメッセージを受信すると(ステップS101)、DNSクエリ・応答送受信部A121aは、DNSサーバアドレス設定テーブルA124aに登録されている外部DNSサーバB1aに、受信したDNSクエリメッセージを転送し（ステップS102）、応答としてDNSサーバB1aからDNSレスポンスメッセージを受信する（ステップS103）。

【００８１】

DNSクエリ・応答送受信部A121aは、受信したDNSレスポンスメッセージから名前解決結果を取り出し、通信方式解決部A122aに渡す。通信方式解決部A122aは、渡された名前解決結果を元に、CUG設定テーブルA125aを参照して、通信相手の種別(暗号化通信対象ノード、通常通信対象ノードのどちらであるか)を判断する（ステップS104）。また、通信相手が暗号化通信対象ノードである場合には、CUG設定テーブルA125aに登録されている暗号化通信路設定情報を把握する。

【００８２】

通信相手が暗号化通信対象ノードである場合、通信方式解決部A122aは、DNSクエリ・応答送受信部A121aから渡された名前解決結果と、CUG設定テーブルA125aから取得した暗号化通信路設定情報とを暗号化通信路設定部A123aに渡す。暗号化通信路設定部A123aは、通信方式解決部A122aから名前解決結果と暗号化通信路設定情報とを受け取ると、これらの情報を暗号化通信路設定テーブルA142aに登録する(S105)。登録後、DNSクエリ・応答送受信部A121aは、外部DNSサーバB1aから受け取った名前解決結果を含むDNSレスポンスメッセージをアプリケーションA11xに送信する(ステップS106)。

【００８３】

以上が、アプリケーションA11xが名前解決要求を行った際のクライアントノードA1の動作である。

【００８４】

次にアプリケーションA11xが通信相手に対してデータパケットを送信した場合の動作について説明する。

【００８５】

アプリケーションA11xは、DNS Proxy部A12aからDNSレスポンスメッセージを受信すると、DNSレスポンスメッセージで通知された名前解決結果に含まれるIPアドレス(すなわち通信相手のIPアドレス)宛にデータパケットを送信する。ここで、送信されたデータパケットはすべてデータ送受信部A14aによってインターセプトされる。

【００８６】

データ送受信部A14aがデータパケットをインターセプトすると、通信暗号化部A141aは、受信したデータパケットの宛先IPアドレスを元に暗号化通信路設定テーブルA142aを参照し、宛先IPアドレスが暗号化通信路対象ノードのIPアドレスとして登録されているか否かをチェックする。そして、暗号化通信路対象ノードの場合は、データパケットに暗号化処理を施した後、送信し、通常通信対象ノードの場合は、データパケットをそのまま送信する。

【００８７】

なお、以上の説明では、DNS Proxy部A12aが外部DNSサーバB1aから通信相手の名前解決結果を受け取った後に通信相手のノード種別を判断する方法を説明したが、本実施の形態では他の方法として、DNS Proxy部A12aが外部DNSサーバB1aに通信相手の名前解決を要求する前に通信相手のノード種別を判断する方法を採ることも可能である。この場合、例えば通信相手のノード種別に応じて、名前解決を要求する(すなわちDNSクエリメッセージを送信する)DNSサーバを変えるといった制御を行うことが可能になるため、暗号化通信を行うグループ専用のDNSサーバを構築できるといった利点がある。

【００８８】

次に本実施の形態の効果について説明する。

【００８９】

従来技術においては、本実施の形態のようにOSのカーネル部が通信暗号化を行う場合、データパケットに含まれる情報から通信相手のノード種別を判断する方式を採っていたため

、暗号化通信対象ノードの識別情報をドメイン名によって指定することが不可能であった。これに対して本実施の形態では、DNS Proxy部A12aが、アプリケーションA11xが通信相手の名前解決を要求する際にDNSサーバB1aと送受信するDNSメッセージをインターセプトし、DNSメッセージに含まれる情報から通信相手のノード種別を判断するため、暗号化通信対象ノードの識別情報をドメイン名によって指定することが可能である。識別情報をドメイン名により指定することで、IPアドレスで指定する場合と異なり、通信相手のIPアドレスが動的に変化する(例えばDHCPでIPアドレスが払い出される場合)状況下でも設定を変更する必要がない。さらに、暗号化通信対象ノードをドメイン名条件(例えばsato.*(前方ラベルがsatoであるFQDNを示す)のようなドメインプレフィックスや、*.biglobe.ne.jp(後方ラベルがbiglobe.ne.jpであるFQDNを示す)のようなドメインサフィックス、*.biglobe.*(biglobeというラベルを含む任意のFQDNを示す）のような条件など）によって指定することも可能であるため、複数のノードから成るグループにおいて設定が共通する暗号化通信路を用いた通信を行う場合には、グループを構成するノードのドメイン名条件を共通化しておくことで（例えば、グループ内ノードのドメインサフィックスを*.myfriends.comとする等）、グループ単位で設定を行うことができ、設定コストを軽減できる。単にグループ単位で設定を行うだけであれば、例えば10.2.1.0/24などのようなIPアドレススコープを利用することも可能だが、グループを構成するノードのIPアドレスが同一のIPアドレススコープに属していなければ、IPアドレススコープをグループの識別情報として利用することは出来ず、任意のノードから自由にグループを構成するということはできない。これに対して、ドメイン名はIPアドレスに依存せずに自由につけることが可能であり、グループを自由に構成することが出来る。

【００９０】

次に本発明の第二の実施の形態について図面を参照して詳細に説明する。

【００９１】

図5を参照すると、本発明の第二の実施の形態は、本発明の第一の実施の形態と比較して、DNS Proxy部A12d内に通信方式解決部およびCUG設定テーブルが含まれず、これらのモジュールがDNSサーバB1dに含まれる点が異なる。本実施の形態においては、アプリケーションA11xの通信相手のノード種別及び通信相手が暗号化通信対象ノードである場合に用いる暗号化通信路の設定情報が、クライアントノードA1d内部ではなく、外部のDNSサーバB1dによって解決される。

【００９２】

以下、本実施の形態について本発明の第一の実施の形態と異なる部分(すなわちDNS Proxy部A12dおよびDNSサーバB1d)を中心に説明する。

【００９３】

まずDNS Proxy部A12dについて説明する。本実施の形態においてDNS Proxy部A12dは、アプリケーションA11xの通信相手の名前解決および通信相手のノード種別(及び通信相手が暗号化通信対象端末の場合は通信相手との通信に用いる暗号化通信路設定情報)解決をDNSサーバB1dに対して要求し、通信相手が暗号化通信対象端末である場合にはDNSサーバB1dが解決した暗号化通信路の設定情報を暗号化通信路設定テーブルA142aに登録する機能を有する。

【００９４】

DNSクエリ・応答送受信部A121dは、外部DNSサーバB1dに対してアプリケーションA11xの通信相手の名前解決を要求する機能に加えて、外部DNSサーバB1dに対してアプリケーションA11xの通信相手のノード種別及び通信相手が暗号化通信対象ノードである場合に通信相手との通信に用いる暗号化通信路の設定情報の解決を要求する機能を持つ。DNSクエリ・応答送受信部A121dは、アプリケーションA11xからDNSクエリメッセージを受信すると、同メッセージをDNSサーバB1dに転送し、応答として受信するDNSレスポンスメッセージの受信処理を行う。DNSサーバB1dから受信するDNSレスポンスメッセージには、アプリケーションA11xの通信相手の名前解決結果に加え、通信相手のノード種別情報が含まれ、更に通信相手が暗号化通信対象ノードである場合には、通信相手との通信に用いる暗号化通信路の

設定情報が含まれる。

【００９５】

DNSレスポンスメッセージによって、通信相手が通常通信対象ノードであると通知された場合および暗号化通信対象ノードであると通知された場合、DNSクエリ・応答送受信部A121dは、受信メッセージに含まれる通信相手の名前解決結果をアプリケーションA11xにDNSレスポンスメッセージによって通知する。また、通信相手が暗号化通信対象ノードであると通知された場合には、DNSクエリ・応答送受信部A121dは、暗号化通信路設定部A123dに対して通信相手の名前解決結果及び通信相手との通信に利用すべき暗号化通信路の設定情報を渡す。暗号化通信路設定部A123dは、本発明の第一の実施の形態における暗号化通信路設定部A123aと同様の機能を有し、DNSクエリ・応答送受信部A121dから受け取った情報を暗号化通信路設定テーブルA142aに登録する。

【００９６】

DNSサーバアドレス設定テーブルA124aには、外部DNSサーバB1dのアドレスが登録されている。

【００９７】

以上がDNS Proxy部A12dの構成である。

【００９８】

次に、DNSサーバB1dについて説明する。DNSサーバB1dは、通常のDNSサーバが持つ名前解決機能に加えて、名前解決要求の対象であるノードの種別を解決する機能を持ち、更にそのノードが暗号化通信対象ノードである場合には、そのノードとの通信に用いる暗号化通信路の設定情報を解決する機能を持つ。

【００９９】

DNSサーバB1dは、DNS応答・クエリ送受信部B11dと名前解決部B12aとアドレス解決用データベースB13aと通信方式解決部B14dとCUG設定データベースB15dとを含む。以下それぞれについて説明する。

【０１００】

DNS応答・クエリ送受信部B11dは、クライアントノードA1dから受け取った名前解決要求(具体的には、受信したDNSクエリメッセージに含まれる名前解決対象のドメイン名やクライアントノードA1dの識別子(例えばIPアドレスやドメイン名など)など)を名前解決部B12aに渡し、名前解決部B12aから名前解決結果(具体的には前記名前解決要求に含まれる情報に加えて、解決結果のIPアドレスなどが含まれる)を受け取る。また、通信方式解決部B14dに前記名前解決結果を渡し、通信方式解決部B14dから名前解決要求の対象のノードの種別情報を受け取る。更に、名前解決要求対象ノードが暗号化通信ノードである場合は、そのノードとの通信に用いる暗号化通信路の設定情報を受け取る。DNS応答・クエリ送受信部B11dは、名前解決部B12a及び通信方式解決部B14dから受け取った情報を元にDNSレスポンスメッセージを作成し、クライアントノードA1dに送信する。

【０１０１】

名前解決部B12aは、DNS応答・クエリ送受信部B11dから名前解決要求を渡されると、アドレス解決用データベースB13aを参照して、名前解決を行い、名前解決結果をDNS応答・クエリ送受信部B11dに渡す。

【０１０２】

アドレス解決用データベースB13aには、ドメイン名とそれに対応するIPアドレスが登録されている。

【０１０３】

通信方式解決部B14dは、DNS応答・クエリ送受信部B11dから名前解決結果を渡されると、CUG設定データベースB15dを参照して、通信相手の種別を解決し、通信相手が暗号化通信対象ノードである場合は、更にそのノードとの通信に用いる暗号化通信路の設定情報を解決する。解決動作の具体例は後述する。前記処理を行った後、解決結果をDNS応答・クエリ送受信部B11dに渡す。

【０１０４】

CUG設定データベースB15dには、暗号化通信対象ノードの識別情報が登録される。この他に通信を行う際に利用する暗号化通信路の設定情報を登録することもできる。なお、これらの情報は図2のテーブル201で示すように登録しておくことが出来る。また、暗号化通信対象ノードの識別情報を、個々のクライアントノードもしくはクライアントノードのグループ毎にCUG設定データベースB15dに登録しておくことも出来る。このような登録方法を採ることによって、同一のノードに対する通信方式の解決要求であってもクライアントノードによって異なる通信方式を解決するといった制御を行うことが可能となる。例えば、あるノードの種別を特定のクライアントノードに対してのみ暗号化通信対象ノードとして解決することによって、特定のクライアントノードからのみ暗号化通信を許可するという制御が可能になる。

【０１０５】

CUG設定データベースB15dの具体例を図6に示す。図6に示すCUG設定データベースB15dは、下記（１）、（２）の2種類のテーブルから構成され、クライアントノード毎あるいはそのグループ毎に暗号化通信対象ノードの識別情報と通信を行う際に利用する暗号化通信路の設定情報が登録されている。

（１）暗号化通信対象ノードの識別情報と通信を行う際に利用する暗号化通信路の設定情報が登録されたテーブル。テーブル502～504が該当する。テーブル502～504には、暗号化通信対象ノードの識別情報がドメイン名の形で登録され、暗号化通信路の設定情報（暗号化通信路仕様）として、通信プロトコル、電子証明書ID、暗号化アルゴリズムが登録されている。

（２）クライアントノードの識別情報と、当該クライアントノードからのDNSクエリメッセージ受信を契機とした通信方式解決の際に参照される上記（１）テーブルの識別子が登録されたテーブル。テーブル501が該当する。テーブル501には、クライアントノードの識別情報がIPアドレスの形で登録されており、当該IPアドレスを持つクライアントノードからのDNSクエリメッセージ受信を契機とした通信方式解決の際に参照されるテーブル502～504の識別子が登録されている。

【０１０６】

以下、DNSサーバB1dが図6に示すCUG設定データベースB15dを保持している場合の、通信方式解決動作の具体例を説明する。

【０１０７】

例えば、IPアドレスが1.2.3.4であるクライアントノードからDNSクエリメッセージを受信した場合、まずテーブル501が参照され、クライアントノード識別情報(IPアドレス：1.2.3.4)が合致する1番目のエントリが引かれる。次に1番目のエントリの登録内容に基づいて、Table ID 1のテーブル、すなわちテーブル502が参照される。クライアントノードが名前解決を要求したドメイン名がkojima.jinji.nec.comである場合は、テーブル502の1番目のエントリが引かれ、通信方式は、[通信ノード種別：暗号化通信対象ノード、通信プロトコル：SSL、電子証明書ID：jinji.nec.com、暗号化アルゴリズム：3DES]のように解決される。

【０１０８】

また、IPアドレスが5.6.7.8であるクライアントノードが上記と同様にkojima.jinji.nec.comの名前解決を要求した場合には、最終的にテーブル503の2番目のエントリが引かれ、通信方式は、[通信ノード種別：暗号化通信対象ノード、通信プロトコル：IPSec、電子証明書ID：soumu-jinji.nec.com、暗号化アルゴリズム：AES]のように上記とは異なる通信方式が解決される。

【０１０９】

さらに、IPアドレスが133.11.23.24であるクライアントノードが上記と同様にkojima.jinji.nec.comの名前解決を要求した場合には、テーブル504が参照されることになるが、そこにはkojima.jinji.nec.comにマッチするエントリが登録されていないため、通信方式は、[通信ノード種別：通常通信対象ノード]のように解決される。

【０１１０】

次に本実施の形態におけるクライアントノードA1d及びDNSサーバB1dの動作を説明する。

【０１１１】

まず、クライアントノードA1dの動作について説明する。クライアントノードA1dの動作は、アプリケーションA11xが通信相手のドメイン名に対する名前解決要求を行った際の動作と、通信相手に対してデータパケットを送信した際の動作に分けられるが、後者については本発明の第一の実施の形態で説明した動作と同一のため、説明を省略する。名前解決要求時の動作については、本発明の第一の実施の形態と比較して外部DNSサーバからDNSレスポンスメッセージを受信した後の動作(図4のステップS104以降)が、本発明の第一の実施の形態と異なる。以下、外部DNSサーバからDNSレスポンスメッセージ受信した後の動作を説明する。

【０１１２】

DNSクエリ・応答送受信部A121dは、DNSサーバB1dからDNSレスポンスメッセージを受信すると、受信したDNSレスポンスメッセージに含まれる名前解決結果を元に、新たにDNSレスポンスメッセージを作成し、アプリケーションA11xに送信する。また、同メッセージに含まれる通信相手のノード種別情報をチェックし、通信相手が暗号通信対象ノードである場合には、DNSサーバB1dから受信したDNSレスポンスメッセージに含まれる通信相手の名前解決結果及びその通信相手との通信に用いる暗号化通信路の設定情報を暗号化通信路設定部A123dに渡す。暗号化通信路A123dは、本発明の第一の実施の形態における動作と同様の手順で、暗号化通信路設定テーブルA142aに暗号通信対象ノードの情報を登録する。

【０１１３】

アプリケーションA11xは、DNSレスポンスメッセージを受信すると、宛先アドレスにDNSレスポンスメッセージによって通知された名前解決結果に含まれるアドレスを指定して、データパケットを送信する。

【０１１４】

次に、DNSサーバB1dの動作を説明する。DNSサーバB1dは、クライアントノードA1dからDNSクエリメッセージを受信すると、クライアントノードA1dの通信相手の名前解決を行う。また、クライアントノードA1dがその通信相手と通信する際に採るべき通信方式を解決する。具体的には、通信相手のノード種別を解決し、そのノードがクライアントノードA1dにとって暗号化通信対象ノードである場合には、更にそのノードとの通信に用いる暗号化通信路の設定情報を解決する。DNSサーバB1dは、以上の解決結果を、DNSレスポンスメッセージによってクライアントノードA1dに送信する。

【０１１５】

次に本実施の形態の効果について説明する。本実施の形態では、暗号化通信対象ノードの識別情報と通信に用いる暗号化通信路の設定情報がDNSサーバB1dによって一元管理される。このため、個々のクライアントノードにおいて前記情報を設定・保持しておく必要がない。特に複数のクライアントノードでグループを構成して通信を行う場合、暗号化通信路の設定情報等に変更があっても、DNSサーバB1dにおいて1度変更を行うだけで済み、DNSサーバB1d上の前記情報をグループ内で効率的に共有することが出来る。

【０１１６】

次に、本発明の第三の実施の形態について図面を参照して詳細に説明する。

【０１１７】

図7を参照すると、本発明の第三の実施の形態は、本発明の第一の実施の形態と比較して、クライアントノードA1gにDNS Proxy部および通信暗号化モジュールが含まれず、これらのモジュールが外部の通信暗号化ノードF1aに含まれる点が異なる。すなわち、本実施の形態は、主に以下の2点において、本発明の第一の実施の形態と異なる。

（１）クライアントノードA1gの通信相手のノード種別(すなわち通信相手が暗号化通信対象ノードであるか通常通信対象ノードであるか)、及び通信相手が暗号化通信対象ノードである場合における当該通信相手との通信に用いる暗号化通信路の設定情報が、通信暗号化ノードF1aによって解決される。

（２）クライアントノードA1gが暗号化通信対象ノードと通信を行う際、通信の暗号化処

理が通信暗号化ノードF1aによって行われる。

【０１１８】

以下、本実施の形態について、本発明の第一の実施の形態と異なる点を中心に説明する。

【０１１９】

まずクライアントノードA1gについて説明する。クライアントノードA１gは、アプリケーションA11xとデータ送受信部A14xとを含む。アプリケーションA11xとデータ送受信部A14xは、本発明の第一の実施の形態の説明におけるものと同様の機能を持つ。但し、データ送受信部A14xには本発明の第一の実施の形態におけるような通信暗号化部及び暗号化通信路設定テーブルはない。また、本実施の形態において、クライアントノードA1gにはDNSサーバとして通信暗号化ノードF1aのアドレスが設定されている。

【０１２０】

次に通信暗号化ノードF1aについて説明する。通信暗号化ノードF1aは、DNS Proxy部F12aとデータ送受信部A14xとを含む。

【０１２１】

まずDNS Proxy部F12aについて説明する。DNS Proxy部F12aは、本発明の第一の実施の形態におけるDNS Proxy部A12aと同様の構成を採り、クライアントノードA1gの通信相手のノード種別を判断し、暗号化通信路の設定情報を暗号化通信路設定テーブルF142aに登録するという機能を持つが、本発明の第一の実施の形態におけるDNS Proxy部A12aとは以下の2点で異なる。

（１）外部クライアントノードA1gからの名前解決要求を受信処理する。

（２）クライアントノードA1gの通信相手が暗号化通信対象ノードである場合には、その通信相手に対する名前解決要求に対して、その通信相手のIPアドレスをインターセプト用アドレスに変換し、名前解決結果として通知する。ここで、インターセプト用アドレスとは、クライアントノードA1gの送信データパケットにおいて宛先アドレスとして指定された場合に、通信暗号化ノードF1aが当該データパケットをインターセプトすることが可能となるアドレスを意味する。具体例としては、通信暗号化ノードF1a自身のIPアドレス等が挙げられるが、詳しくは後述する。なお、後述するようにインターセプト用アドレスとして通信相手のIPアドレスを直接利用する場合もあり、その場合は上記の通信相手のIPアドレスからインターセプト用アドレスへの変換後も、名前解決結果として通信相手のIPアドレスが通知されることになる。

【０１２２】

以下、DNS Proxy部F12aを構成する各モジュールについて説明する。

【０１２３】

DNSクエリ・応答送受信部F121aは、DNSレスポンス・クエリメッセージの送受信を外部クライアントノードA1gに対して行うという点以外は、本発明の第一の実施の形態におけるDNSクエリ・応答送受信部A121aと同様の機能を持つ。

【０１２４】

通信方式解決部F122aは、本発明の第一の実施の形態における通信方式解決部A122aと同様の機能を持つ。

【０１２５】

暗号化通信路設定部F123aは、本発明の第一の実施の形態における暗号化通信路設定部A123aと比較して、通信方式解決部F122aから渡された名前解決結果に含まれるクライアントノードA1gの通信相手のIPアドレスを、インターセプト用アドレスへマッピングする点が異なる。具体的な動作は以下のとおりである。

【０１２６】

暗号化通信路設定部F123aは、通信方式解決部F122aから名前解決結果を渡されると、暗号化通信路設定テーブルF142aを参照して他の通信セッションで使用されていないインターセプト用アドレスを選択し、名前解決結果に含まれるクライアントノードA1gの通信相手のIPアドレスを、前記インターセプト用アドレスへマッピングし、前記インターセプト用アドレスをDNSクエリ・応答送受信部F121aに通知する。また、選択したインターセプト用

アドレスと通信方式解決部F122aから渡された名前解決結果およびクライアントノードA1gの通信相手との通信に利用すべき暗号化通信路の設定情報との対応関係を暗号化通信路設定テーブルF142aに登録する。

【０１２７】

DNSサーバアドレス設定テーブルA124aには、本発明の第一の実施の形態におけるDNSサーバアドレス設定テーブルA124aと同様の情報が登録されている。

【０１２８】

CUG設定データベースF125aには、本発明の第一の実施の形態におけるCUG設定テーブルA125aと同様に暗号化通信対象ノード(CUG参加ノード)の識別情報と通信を行う際に利用する暗号化通信路の設定情報が登録され、通信方式解決部F122aがクライアントノードA1gの通信相手の種別を判断する際に参照される。また、CUG設定データベースF125aは、本発明の第一の実施の形態におけるCUG設定テーブルA125aと同様に、暗号化通信対象ノード毎にノード識別情報と暗号化通信路の設定情報を登録しておくことが可能であり、複数の暗号化通信対象ノードをまとめて一つのグループとして扱い、グループ毎にノード識別情報と暗号化通信路の設定情報を登録しておくことも可能である。さらに、CUG設定データベースF125aは、本発明の第二の実施の形態におけるCUG設定データベースB15dと同様に、暗号化通信対象ノードの識別情報と通信を行う際に利用する暗号化通信路の設定情報の情報をクライアントノードもしくはクライアントノードのグループ毎に登録しておくことも可能であり、その場合、例えば図6のような形で情報が登録される。

【０１２９】

以上がDNS Proxy部F12aの構成である。

【０１３０】

次に、データ送受信部A14xの通信暗号化部F141a及び暗号化通信路設定テーブルF142aについて説明する。

【０１３１】

暗号化通信路設定テーブルF142aには、クライアントノードA1gの通信相手の名前解決結果(通信相手のIPアドレスなど)及び前記通信相手との通信に用いる暗号化通信路の設定情報と、それらに対応するインターセプト用アドレスが登録される。暗号化通信路設定テーブルF142aは、暗号化通信路設定部F123aがクライアントノードA1gの通信相手のIPアドレスを、インターセプト用アドレスへマッピングする際、及び通信暗号化部F141aが通信の暗号化処理を行う際に参照される。図8に暗号化通信路設定テーブルF142aの例を示す。図8に示した暗号化通信路設定テーブル601では、名前解決結果に含まれる情報として、クライアントノードA1gの通信相手のIPアドレス及びドメイン名が、対応するインターセプト用アドレス毎に登録されている。

【０１３２】

通信暗号化部F141aは、クライアントノードA1が暗号化通信対象ノードに対して送信するデータパケットの暗号化処理を行う。以下、暗号化処理の具体的手順について説明する。

【０１３３】

クライアントノードA1gが暗号化通信対象ノードと通信を行う場合、クライアントノードA1gから送信されるデータパケットの宛先アドレスには、インターセプト用アドレスが指定されており(暗号化通信対象ノードに対する名前解決要求に対しては、DNS Proxy部F12aによりインターセプト用アドレスが名前解決結果として通知されるため)、前記データパケットは全て通信暗号化ノードF1aがインターセプトすることになる。インターセプトされたデータパケットは通信暗号化部F141aに渡される。通信暗号化部F141aは、インターセプトしたデータパケットの宛先アドレスを元に暗号化通信路設定テーブルF142aを参照し、宛先インターセプト用アドレスと対応付けられている通信相手のIPアドレス及びその通信相手との通信に利用する暗号化通信路の設定情報を把握する。そして、把握した暗号化通信路の設定情報に従ってインターセプトしたデータパケットを暗号化し、クライアントノードA1gの通信相手に送信する。

【０１３４】

以下、上記で説明した通信暗号化処理の具体例を説明する。具体例としては、データ送受信部A14xが暗号化通信路設定テーブルF142aとして図8に示したテーブル601を保持しているケースを想定し、通信暗号化ノードF1aが、クライアントノードA1gの送信した宛先アドレスfe80::3090のデータパケットをインターセプトした場合の例を説明する。

【０１３５】

通信暗号化部F141aは、まず暗号化通信路設定テーブルF142aを参照して、宛先アドレスfe80::3090に該当するエントリを把握する。この場合、テーブル601の2番目のエントリが該当し、その結果、通信暗号化部F141aは通信に利用する暗号化通信路の設定情報として、通信プロトコル：SSL、電子証明書ID：10、暗号化アルゴリズム：3DESを取得する。次に通信暗号化部F141aは、インターセプトしたデータパケットの宛先アドレスを、fe80::3090から通信相手のIPアドレスであるaa91::1001に書き換え、暗号化通信路の設定情報に従って、3DESアルゴリズムで暗号化した後、SSLプロトコルで通信相手に送信する。

【０１３６】

以上が、通信暗号化部F141aによる通信暗号化処理の具体的手順である。

【０１３７】

次に、インターセプト用アドレスとして利用できるIPアドレスについて説明する。

【０１３８】

インターセプト用アドレスとしては、例えば以下の二つのアドレスが利用できる。

（１）通信暗号化ノードF1a自身のIPアドレス

（２）クライアントノードA1gが属するサブネットのアドレス範囲に含まれない任意のアドレス

【０１３９】

（１）の通信暗号化ノードF1a自身のIPアドレスをインターセプト用アドレスとして利用する場合、通信暗号化ノードF1aには複数のIPアドレスが割り当てられていることが必要となる。その理由は、通信暗号化ノードF1aは、クライアントノードA1gが送信したデータパケットの宛先アドレスに指定されているインターセプト用アドレスによってクライアントノードA1gの通信相手を識別するため、同時に複数の通信相手もしくはクライアントノードの利用を想定する場合には、複数のインターセプト用アドレスを使い分けることが必要になるためである。また、インターセプト用アドレスが多くあるほど、より多くの通信相手もしくはクライアントノードの利用が可能となるため、通信暗号化ノードF1aにはできるだけ多くのIPアドレスが割り当てられている方が都合が良い。

【０１４０】

（２）のクライアントノードA１gが属するサブネットのアドレス範囲に含まれない任意のアドレスをインターセプト用アドレスとして利用する場合、通信暗号化ノードF1aはクライアントノードA1gのデフォルトゲートウェイとなっている必要がある。デフォルトゲートウェイとなることで、クライアントノードA1gが自身の属するサブネットのアドレス範囲に含まれないアドレス宛にデータパケットを送信した場合、そのデータパケットはルーティング処理のために通信暗号化ノードF1aを経由することになる。クライアントノードA1gの通信相手がクライアントノードA1gの属するサブネット外に存在する場合は、通信相手のIPアドレスを直接インターセプト用アドレスとして利用することが可能である。

【０１４１】

次に、本実施の形態において、クライアントノードA1gが通信相手の名前解決を要求してから、その通信相手と通信を行うまでの通信暗号化ノードF1aの動作を説明する。

【０１４２】

通信暗号化ノードF1aの動作は、クライアントノードA1gからDNSクエリを受信した際の動作とクライアントノードA1gが送信したデータパケットをインターセプトした場合の動作に分けられる。

【０１４３】

まず、図4を参照してクライアントノードA1gからＤＮＳクエリを受信した際の動作について説明する。

【０１４４】
通信暗号化ノードF1aがクライアントノードA1gからDNSクエリメッセージを受信する(ステップS101)と、DNSクエリ・応答送受信部F121aがDNSサーバアドレス設定テーブルF124aに登録されている外部DNSサーバB1aに、受信したDNSクエリメッセージを送信し（ステップS102）、応答としてDNSサーバB1aからDNSレスポンスメッセージを受信する（ステップS103）。

【０１４５】
DNSクエリ・応答送受信部F121aは、受信したDNSレスポンスメッセージから名前解決結果を取り出し、通信方式解決部F122aに渡す。

【０１４６】
通信方式解決部F122aは、渡された名前解決結果を元に、CUG設定データベースF125aを参照して、通信相手のノード種別(暗号化通信対象ノード、通常通信対象ノードのどちらであるか)を判断する（ステップS104）。その後の動作は通信相手の種別により異なる。

【０１４７】
まず、通信相手が通常通信対象ノードである場合について説明する。この場合、通信方式解決部F122aからDNSクエリ・応答送受信部F121aに判断結果が通知され、DNSクエリ・応答送受信部F121aが、DNSサーバB1aから通知された名前解決結果を元に新たにDNSレスポンスメッセージを作成し、クライアントノードA1gに送信する(ステップS106)。

【０１４８】
クライアントノードA1gは、DNSレスポンスメッセージを受信すると、受信したDNSレスポンスメッセージにより通知された通信相手のIPアドレスを宛先アドレスとしてデータパケットを送信する。この場合、クライアントノードA1gが送信したデータパケットは、通信暗号化ノードF1aを経由せずに通信相手に直接送信され、通信相手とは通常の通信が行われることになる。

【０１４９】
次に、通信相手が暗号化通信対象ノードである場合について説明する。この場合、通信方式解決部F122aは、クライアントノードA1gの通信相手との通信に利用する暗号化通信路の設定情報をCUG設定データベースF125aから把握し、DNSクエリ・応答送受信部F121aから渡された名前解決結果と共に暗号化通信路設定部F123aに渡す。

【０１５０】
暗号化通信路設定部F123aは、名前解決結果及び暗号化通信路の設定情報を受け取ると、暗号化通信路設定テーブルF142aを参照し、クライアントノードA1gの通信相手のIPアドレスを、他の通信セッションで使用されていないインターセプト用アドレスへマッピングする。暗号化通信路設定部F123aは、マッピングしたインターセプト用アドレスを通信方式解決部F122aに通知する。また、暗号化通信路設定部F123aは、インターセプト用アドレスと、通信方式解決部F122aから渡された名前解決結果及び通信相手との通信に利用する暗号化通信路設定情報の対応関係を暗号化通信路設定テーブルF142aに登録する(ステップS105)。

【０１５１】
通信方式解決部F122aは、暗号化通信路設定部F123aから渡されたインターセプト用アドレスをDNSクエリ・応答送受信部F121aに渡す。

【０１５２】
DNSクエリ・応答送受信部F121aは、通信方式解決部F122aからインターセプト用アドレスを通知されると、外部DNSサーバB1aから渡された名前解決結果に含まれる通信相手のアドレスをインターセプト用アドレスに書き換え、DNSレスポンスメッセージを作成し、クライアントノードA1gに送信する。つまり、クライアントノードA1gには、通信相手のドメイン名に対する名前解決結果として、暗号化通信路設定部F123aが選択したインターセプト用アドレスが通知されることになる(ステップS106)。

【０１５３】
クライアントノードA1gは、DNSレスポンスメッセージを受信すると、名前解決結果に含ま

れるインターセプト用アドレスを宛先アドレスに指定してデータパケットを送信する。この結果、前記データパケットは通信暗号化ノードF1aによってインターセプトされ、暗号化処理が行われることになる。

【０１５４】

以上が、通信暗号化ノードF1aがクライアントノードA1gからDNSクエリを受信した際の動作である。

【０１５５】

次に通信暗号化ノードF1aがクライアントノードA1gの送信したデータパケットをインターセプトした場合の動作について説明する。

【０１５６】

通信暗号化ノードF1aが、クライアントノードA1gが送信したデータパケットをインターセプトすると、通信暗号化部F141aは、データパケットの宛先アドレス(インターセプト用アドレスが指定されている)を基に暗号化通信路設定テーブルF142aを参照し、クライアントノードA1gの通信相手との通信に利用すべき暗号化通信路の設定情報及び通信相手のIPアドレスを取得する。そして、通信暗号化部F141aは、取得した暗号化通信路の設定情報を利用して、暗号・復号化処理部F1411aにおいて、インターセプトしたデータパケットに対して暗号化処理を行い、且つデータパケットの宛て先アドレスに通信相手のIPアドレスを設定して、通信相手に対して送信する。

【０１５７】

なお、以上の説明では通信相手のノード種別と、通信相手が暗号化通信対象端末であった場合にその通信相手との通信に利用する暗号化通信路設定情報の解決を通信暗号化ノードF1aの内部で行う構成について説明したが、本実施の形態において、本発明の第二の実施の形態と同様に、上記解決をDNSサーバB1aで行う構成を採ることも可能である。この場合、DNSサーバB1aの構成は、本発明の第二の実施の形態における図5に示したDNSサーバB1dと同様の構成を採り、通信暗号化ノードF1aは、図9に示す構成を採る。この場合、DNSクエリ・応答送受信部F121aは、本発明の第二の実施の形態におけるDNSクエリ・応答送受信部A121dと同様の機能を持つ。

【０１５８】

図9に示される通信暗号化ノードF1aは、カーネル部に設けられたデータ送受信部A14xと、図示しないクライアントノード上のアプリケーションが他のノード装置のIPアドレスを解決するために図示しない名前解決サーバに送信する名前解決クエリ及びその応答である名前解決応答を中継する名前解決プロキシ部F12aとを備える。

【０１５９】

データ送受信部A14xは、通信相手IPアドレスとインターセプト用アドレスと暗号化通信路設定情報との対応を保持する暗号化通信路設定テーブルF142aと、前記アプリケーションより送信された宛先アドレスにインターセプト用アドレスが設定されたデータパケットを受信し、前記データパケットの宛先アドレスに設定されたインターセプト用アドレスに対応する通信相手IPアドレス及び暗号化通信路設定情報を暗号化通信路設定テーブルF142aから読み出し、前記データパケットの宛先アドレスに前記読み出した通信相手IPアドレスを設定したデータパケットを、前記読み出した暗号化通信路設定情報に従って暗号化して送信する通信暗号化部F141aとを備える。

【０１６０】

図示しない名前解決サーバは、名前解決に関連する機能に加えて、暗号化通信対象ノードを特定するドメイン名条件と暗号化通信路設定情報との対応を保持する設定テーブルと、前記名前解決クエリまたは前記名前解決応答に含まれる前記他のノード装置のドメイン名が前記設定テーブルに保持された何れかのドメイン名条件にマッチするかどうかを判定する通信方式解決部と、前記マッチしたドメイン名条件に対応する暗号化通信路設定情報を前記名前解決応答に付加して送信する名前解決応答・クエリ送受信部とを備えている。そして、名前解決プロキシ部F12aは、前記暗号化通信路設定情報が付加された前記名前解決応答を前記名前解決サーバから受信したときに、前記暗号化通信路設定情報と前記名前

解決応答で解決された前記他のノード装置のIPアドレスと他の通信セッションで使用されていないインターセプト用アドレスとの対応を暗号化通信路設定テーブルF142aに登録する暗号化通信路設定部F123a、前記名前解決サーバから受信した名前解決応答に含まれる前記他のノード装置のIPアドレスに対応するインターセプト用アドレスを名前解決応答として前記アプリケーションに送信する名前解決クエリ・応答送受信部F121aとを備える。

【０１６１】

次に本実施の形態の効果について説明する。本実施の形態では、通信相手の種別判断及び、暗号化通信対象ノードに対する通信暗号化処理が各クライアントノード内ではなく、外部の通信暗号化ノードで行われる。このため、クライアントノードに通信暗号化モジュールをインストールできない場合でも利用することが可能である。さらに、クライアントノード内で通信相手の種別判断及び、暗号化通信対象ノードに対する通信暗号化処理を行う場合と比較して、クライアントノードにかかる負荷が軽減されるため、計算能力が比較的低いノード(例えば携帯電話やPDA等)でも利用することが出来る。

【０１６２】

以上本発明の実施の形態について説明したが、本発明は以上の実施の形態にのみ限定されず、その他各種の付加変更が可能である。また、本発明のクライアントノード装置、通信暗号化ノード装置、名前解決サーバは、その有する機能をハードウェア的に実現することは勿論、コンピュータとプログラムとで実現することができる。プログラムは、磁気ディスクや半導体メモリ等のコンピュータ可読記録媒体に記録されて提供され、コンピュータの立ち上げ時などにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータを前述した各実施の形態におけるクライアントノード装置、通信暗号化ノード装置、名前解決サーバとして機能させる。

【図面の簡単な説明】

【０１６３】

【図１】本発明の第一の実施の形態の構成を示すブロック図

【図２】本発明の第一の実施の形態のCUG設定テーブルの例を示す図

【図３】本発明の第一の実施の形態の暗号化通信路設定テーブルの例を示す図

【図４】本発明の第一及び第三の実施の形態のDNS Proxy部の名前解決要求受け付け時の動作を示す流れ図

【図５】本発明の第二の実施の形態の構成を示すブロック図

【図６】本発明の第二の実施の形態のCUG設定データベースの例を示す図

【図７】本発明の第三の実施の形態の構成を示すブロック図

【図８】本発明の第三の実施の形態の暗号化通信路設定テーブルの例を示す図

【図９】本発明の第三の実施の形態の変形例におけるクライアントノードの構成を示すブロック図

【図１０】通信暗号化モジュールを利用する従来の暗号通信システムの構成を示す図

【図１１】OSのカーネル部の通信暗号化機能を利用する従来の暗号通信システムの構成を示す図

【符号の説明】

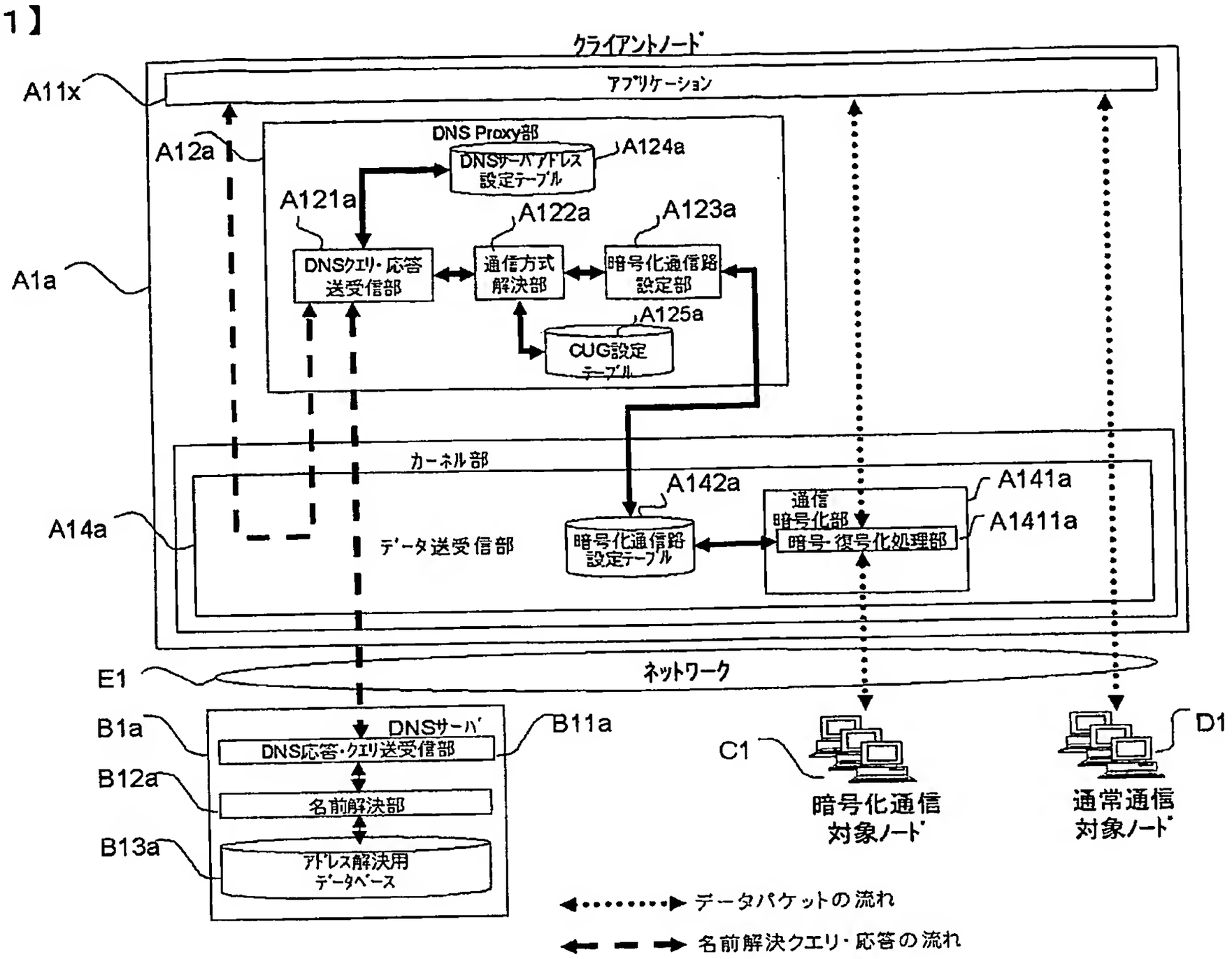
【０１６４】

A1a クライアントノード
A1d クライアントノード
A1g クライアントノード
A1x クライアントノード
A1y クライアントノード
A11x アプリケーション
A12a DNS Proxy部
A12d DNS Proxy部
A121a DNSクエリ・応答送受信部
A121d DNSクエリ・応答送受信部

A122a 通信方式解決部
A123a 暗号化通信路設定部
A123d 暗号化通信路設定部
A124a DNSサーバアドレス設定テーブル
A125a CUG設定テーブル
A13x 通信暗号化モジュール
A131x 通信暗号化部
A1311x 暗号・復号化処理部
A1312x アドレス変換部
A132x 暗号化通信路設定テーブル
B1a DNSサーバ
B1b DNSサーバ
B11a DNS応答・クエリ送受信部
B11d DNS応答・クエリ送受信部
B12a 名前解決部
B13a アドレス解決用データベース
B14d 通信方式解決部
B15d CUG設定データベース
C1 暗号化通信対象ノード
D1 通常通信対象ノード
E1 ネットワーク
F1a 通信暗号化ノード
F12a DNS Proxy部
F121a DNSクエリ・応答送受信部
F122a 通信方式解決部
F123a 暗号化通信路設定部
F125a CUG設定テーブル

【書類名】図面
【図１】

【図１】



【図２】

【図２】

201

CUG識別情報	暗号化通信路設定情報		
ドメイン名	通信プロトコル	電子証明書ID	暗号化アルゴリズム
…	…	…	…
taro.nec.co.jp	SSL	10	3DES
jiro.biglobe.ne.jp	IPSec	15	AES
*.myfriends.com	SSL	11	DES
*.myfamily.com	IPSec	12	3DES
sato.*	SSL	13	DES
*.satofamily. *	SSL	14	AES
…	…	…	…

【図３】

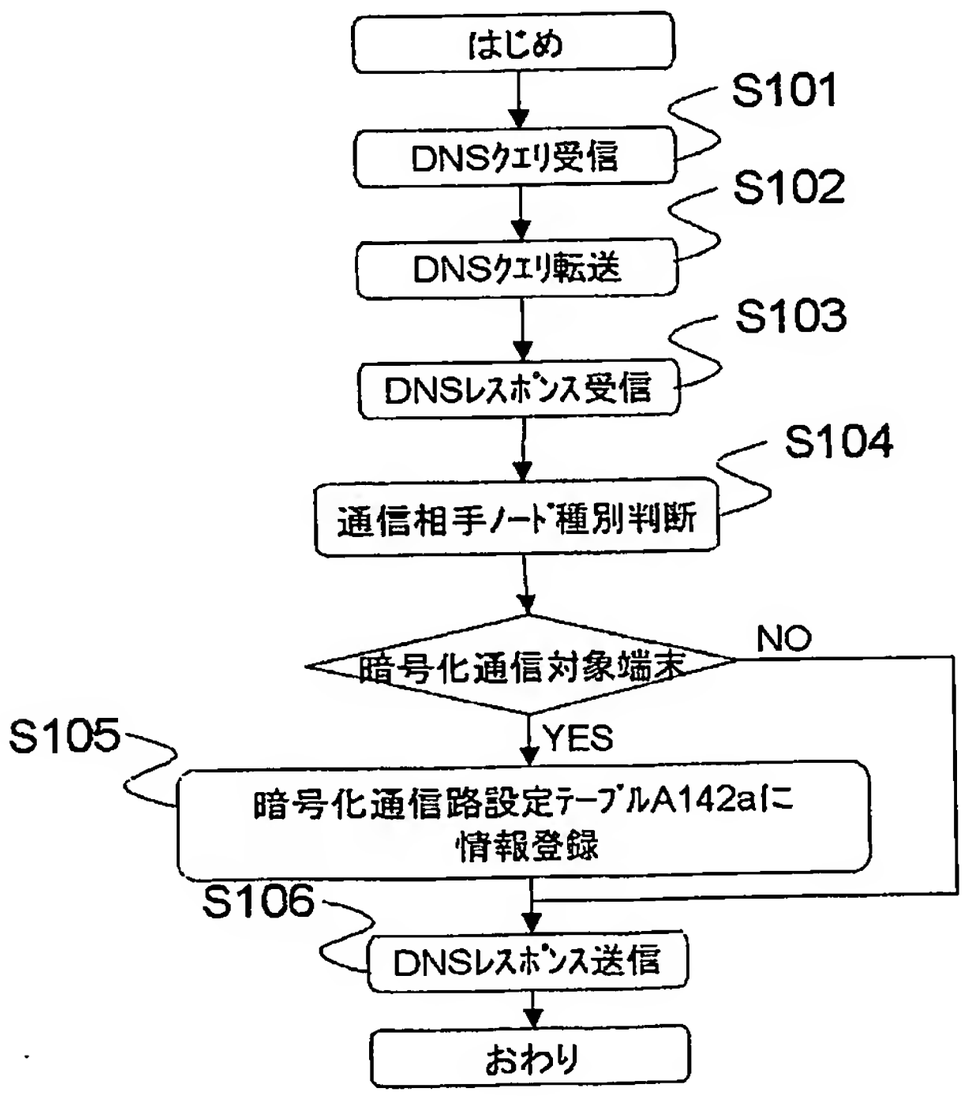
【図３】

301

通信相手IPｱﾄﾞﾚｽ	暗号化通信路設定情報		
	通信ﾌﾟﾛﾄｺﾙ	電子証明書ID	暗号化ｱﾙｺﾞﾘｽﾞﾑ
…	…	…	…
133.11.64.24	IPSec	10	3DES
19.23.43.13	IPSec	15	AES
1.3.3.2	IPSec	11	DES
…	…	…	…

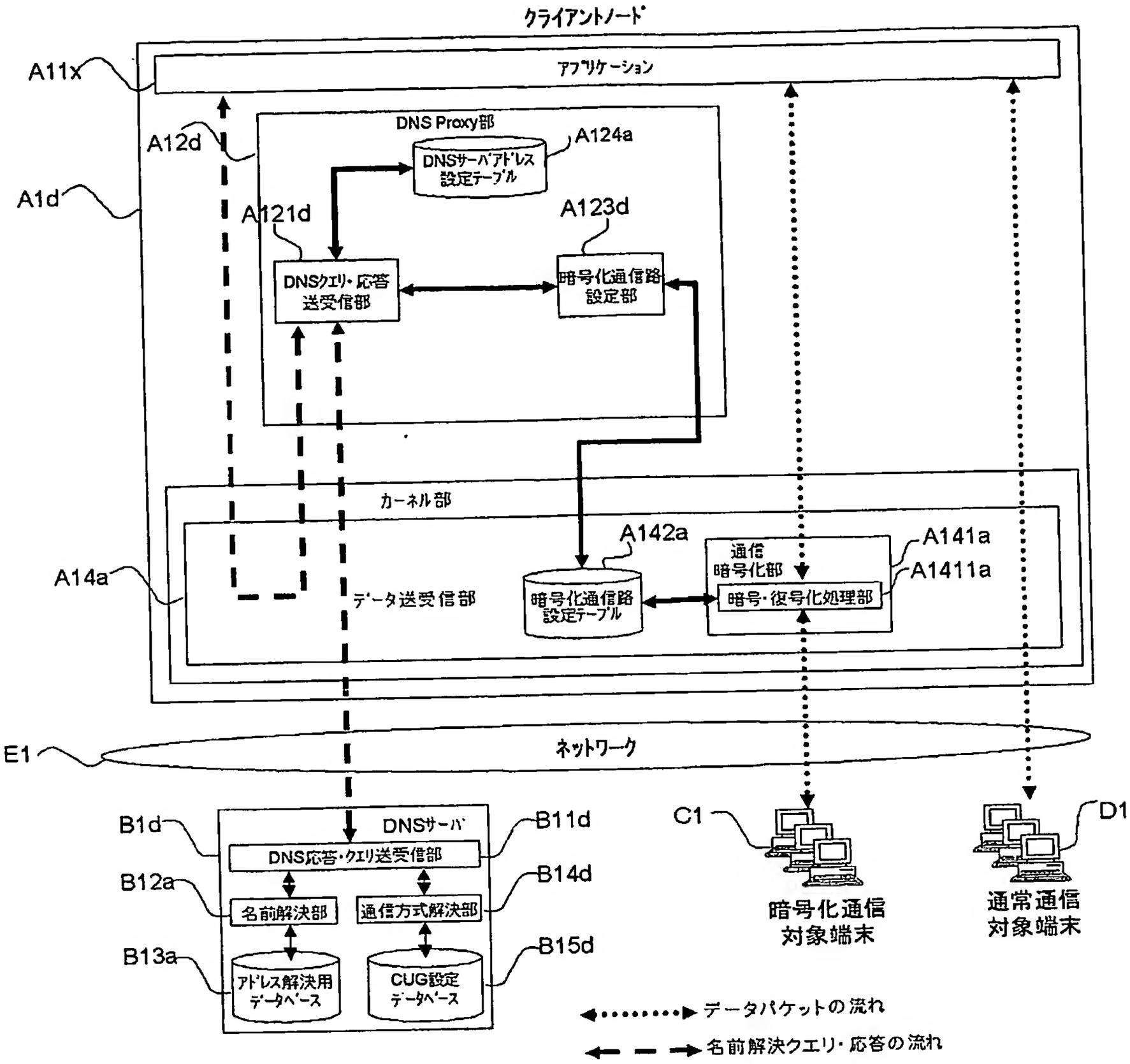
【図４】

【図４】



【図５】

【図５】


クライアントノード
A11x
アプリケーション
DNS Proxy部
A12d
A124a
DNSサーバアドレス設定テーブル
A1d
A121d
A123d
DNSクエリ・応答送受信部
暗号化通信路設定部
カーネル部
A142a
A141a
A1411a
通信暗号化部
A14a
データ送受信部
暗号化通信路設定テーブル
暗号・復号化処理部
E1
ネットワーク
B1d
DNSサーバ
B11d
DNS応答・クエリ送受信部
B12a
B14d
名前解決部
通信方式解決部
B13a
B15d
アドレス解決用データベース
CUG設定データベース
C1
D1
暗号化通信対象端末
通常通信対象端末
データパケットの流れ
名前解決クエリ・応答の流れ

【図６】

【図６】

501

ｸﾗｲｱﾝﾄﾉｰﾄﾞ識別情報	Table ID
IPｱﾄﾞﾚｽ	
1.2.3.4	1
5.6.7.8	2
…	…
133.11.23.24	n
…	…

502

Table ID:1			
CUG識別情報	暗号化通信路仕様		
ﾄﾞﾒｲﾝ名	通信ﾌﾟﾛﾄｺﾙ	電子証明書ID	暗号化ｱﾙｺﾞﾘｽﾞﾑ
*.jinji.nec.com	SSL	jinji.nec.com	3DES
*.soumu.nec.com	IPSec	jinji-soumu.nec.com	AES
*.keiri.nec.com	IPSec	jinji-keiri.nec.com	DES
…	…	…	…

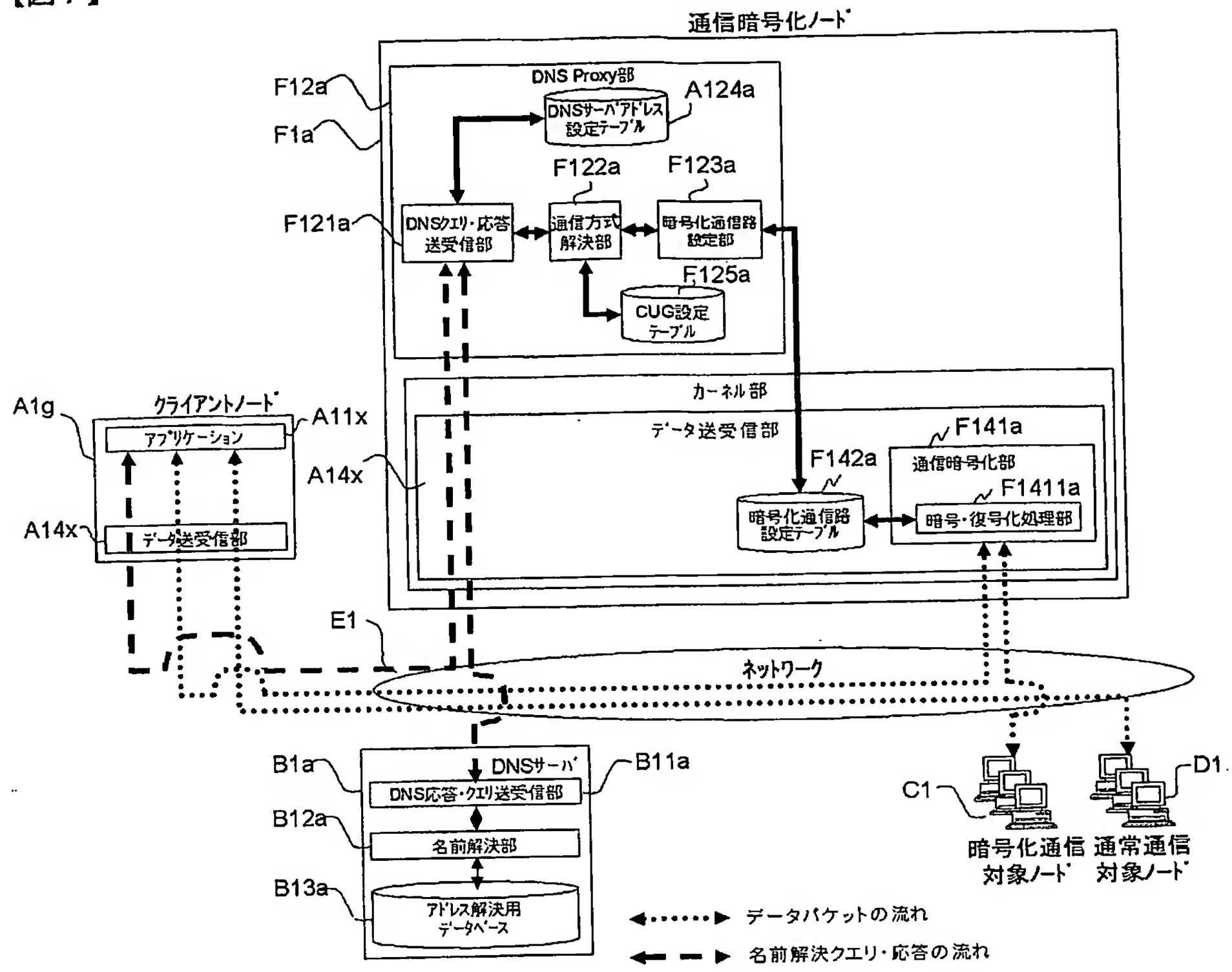
503

Table ID:2			
CUG識別情報	暗号化通信路仕様		
ﾄﾞﾒｲﾝ名	通信ﾌﾟﾛﾄｺﾙ	電子証明書ID	暗号化ｱﾙｺﾞﾘｽﾞﾑ
*.soumu.nec.com	SSL	soumu.nec.com	3DES
*.jinji.nec.com	IPSec	soumu-jinji.nec.com	AES
*.keiri.nec.com	IPSec	jinji-keiri.nec.com	DES
…	…	…	…

504

Table ID:n			
CUG識別情報	暗号化通信路仕様		
ﾄﾞﾒｲﾝ名	通信ﾌﾟﾛﾄｺﾙ	電子証明書ID	暗号化ｱﾙｺﾞﾘｽﾞﾑ
*.satofamily.com	SSL	satofamily	3DES
*.suzukifamily.com	IPSec	sato-suzukifamily	AES
…	…	…	…

【図７】



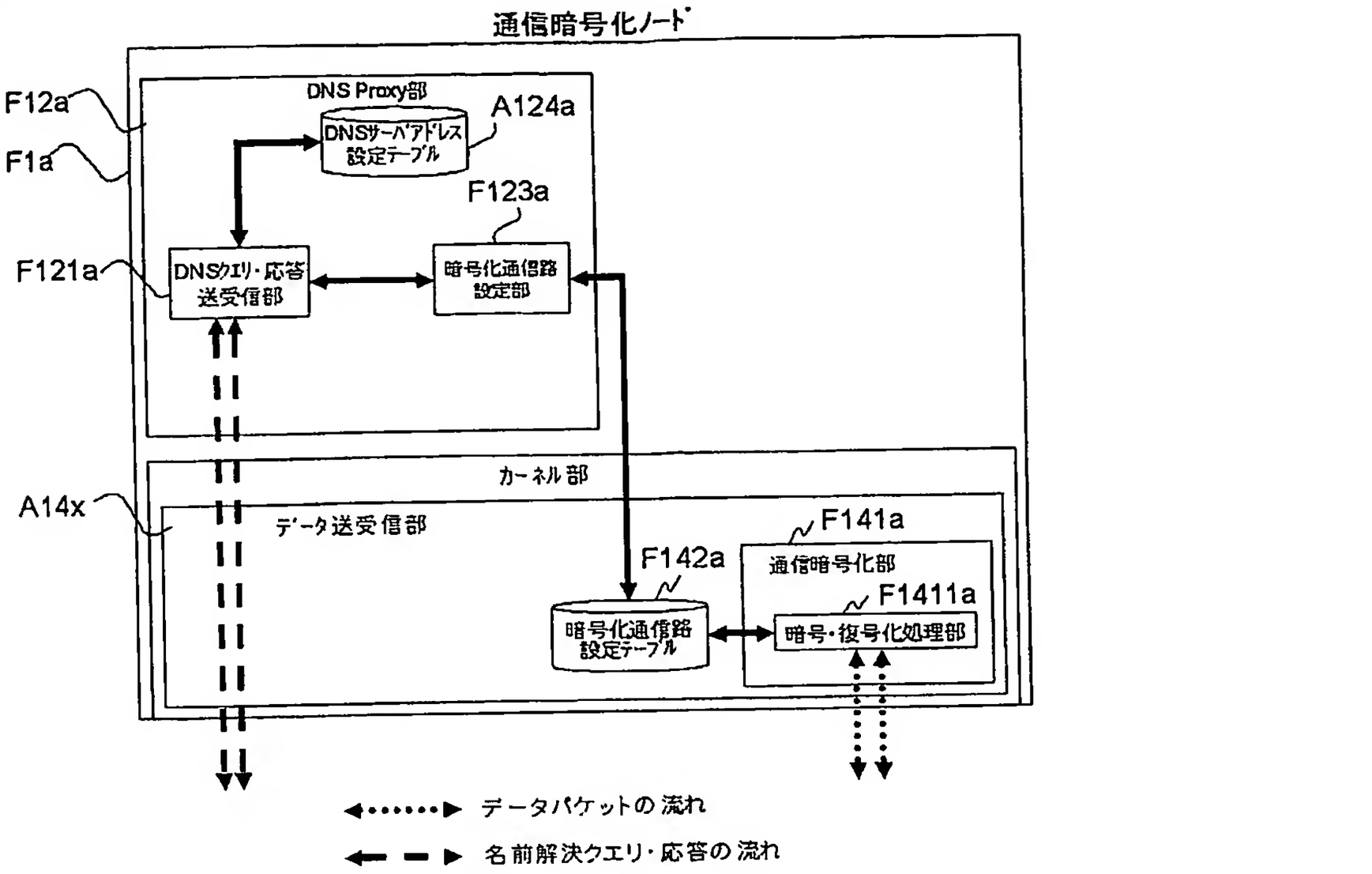
【図８】

601

インターセプト用アドレス	通信相手IPアドレス	暗号化通信路設定情報		
		通信プロトコル	電子証明書ID	暗号化アルゴリズム
…	…	…	…	…
fe80::3090	aa91::1001	SSL	10	3DES
fe81::3091	bb92::1002	IPSec	15	AES
…	…	…	…	…

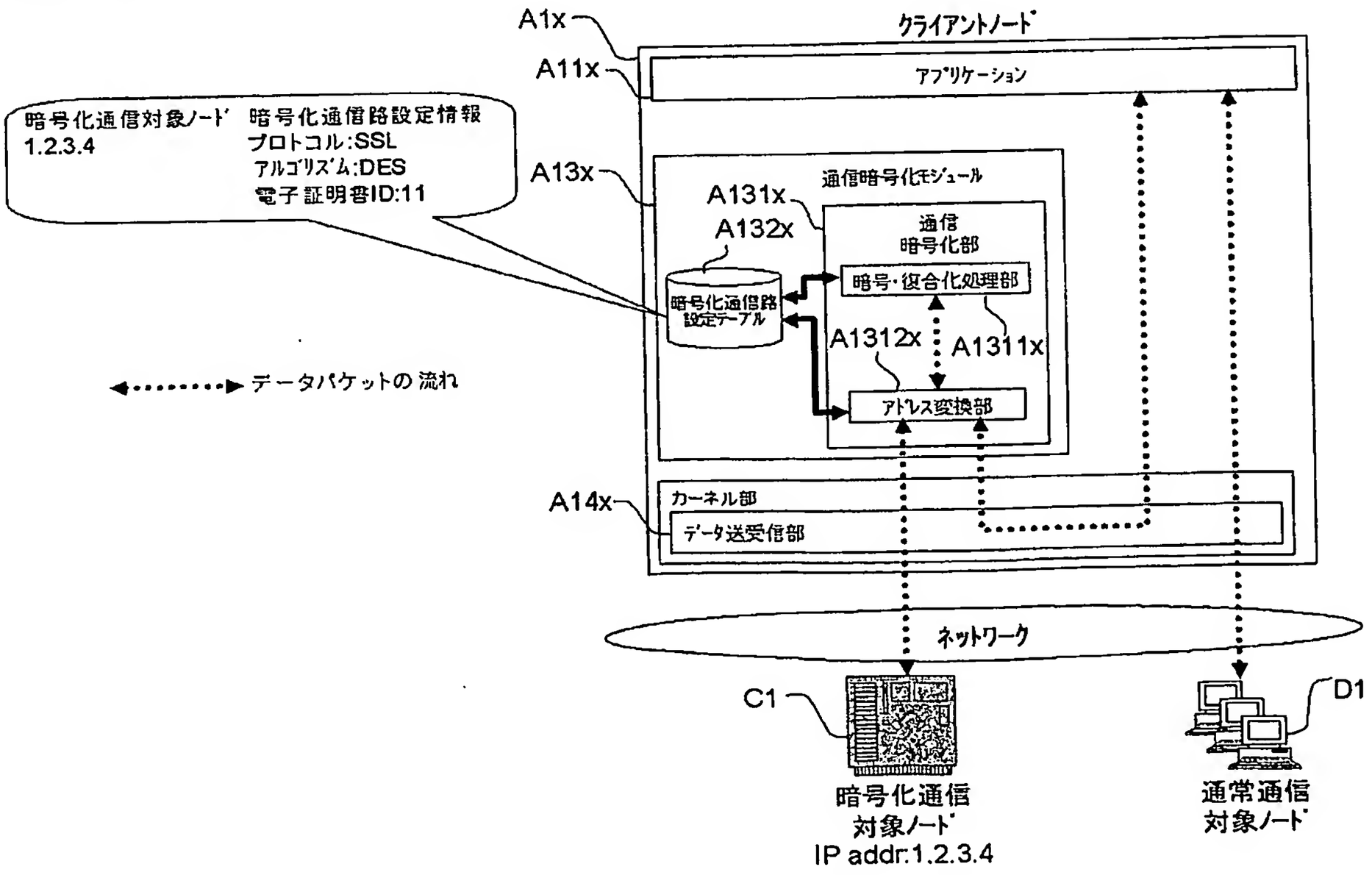
【図９】

【図９】

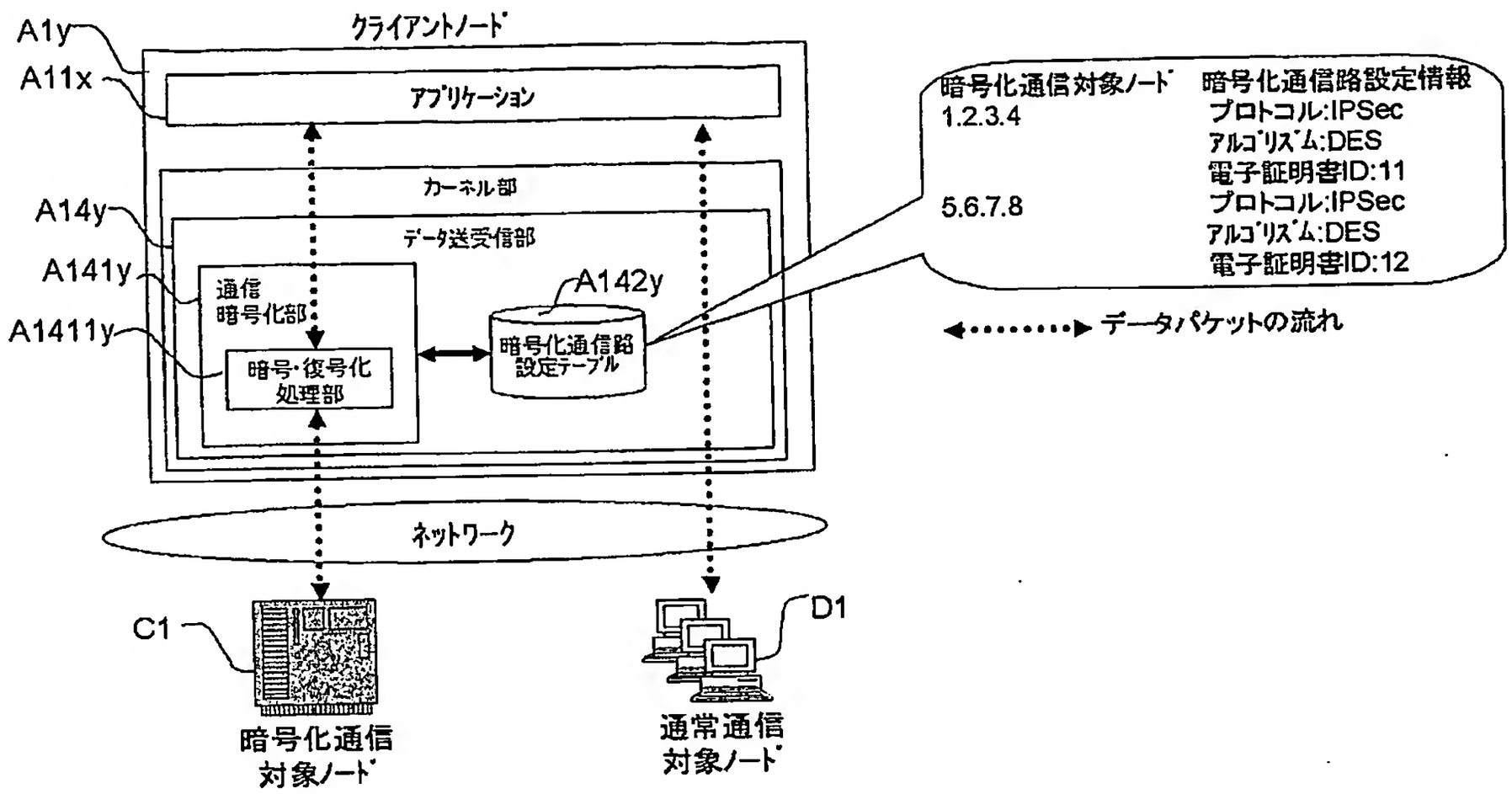

通信暗号化ノード
DNS Proxy部
A124a
DNSサーバアドレス設定テーブル
F12a
F1a
F123a
F121a
DNSクエリ・応答送受信部
暗号化通信路設定部
カーネル部
A14x
データ送受信部
F141a
F142a
通信暗号化部
F1411a
暗号化通信路設定テーブル
暗号・復号化処理部
データパケットの流れ
名前解決クエリ・応答の流れ

【図１０】

【図１０】


A1x
クライアントノード
A11x
アプリケーション
暗号化通信対象ノード
1.2.3.4
暗号化通信路設定情報
プロトコル:SSL
アルゴリズム:DES
電子証明書ID:11
A13x
通信暗号化モジュール
A131x
A132x
通信暗号化部
暗号化通信路設定テーブル
暗号・復合化処理部
A1312x
A1311x
アドレス変換部
A14x
カーネル部
データ送受信部
ネットワーク
C1
D1
暗号化通信対象ノード
IP addr:1.2.3.4
通常通信対象ノード
データパケットの流れ

【図１１】


A1y
クライアントノード
A11x
アプリケーション
カーネル部
A14y
データ送受信部
A141y
通信
暗号化部
A1411y
暗号・復号化
処理部
A142y
暗号化通信路
設定テーブル
ネットワーク
C1
暗号化通信
対象ノード
D1
通常通信
対象ノード
暗号化通信対象ノード
暗号化通信路設定情報
1.2.3.4
プロトコル:IPSec
アルゴリズム:DES
電子証明書ID:11
5.6.7.8
プロトコル:IPSec
アルゴリズム:DES
電子証明書ID:12
データパケットの流れ

【書類名】要約書
【要約】
【課題】　OSが提供する通信暗号化機能を利用して複数の通信相手と暗号化通信を行う場合の暗号化通信対象ノードの設定を、ドメイン名で行えるようにする。
【解決手段】　DNS Proxy部A12aは、暗号化通信対象ノードのドメイン名をCUG設定テーブルA125aに保持しており、アプリケーションA11xからDNSサーバB1aに出される通信相手ノードに対する名前解決要求をインターセプトし、CUG設定テーブルA125aを参照して通信相手が暗号化通信対象ノードか否かを判断し、暗号化通信対象ノードであれば、名前解決された通信相手のIPアドレスを暗号化通信路設定テーブルA142aに登録する。アプリケーションA11xがそのIPアドレス宛にデータパケットを送出すると、データ送受信部A14aでインターセプトされ、暗号化通信路設定テーブルA142aに登録されたIPアドレス宛のデータパケットは通信暗号化部A141aで暗号化され、通信相手に送信される。
【選択図】　図1

特願２００４－００６５４２

出願人履歴情報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社

出証番号　出証特２００４－３０９１０５５